LUISS Università Guido Carli

Dipartimento di Scienze Politiche *Cattedra di Diritto dell'Informazione della Comunicazione (c.p.)*

I CRIMINI INFORMATICI, LA DISCIPLINA NELL'ORDINAMENTO ITALIANO E LA COOPERAZIONE INTERNAZIONALE

RELATORE

Chiar.mo Prof. Pietro Santo Leopoldo Falletta

CANDIDATO

Ludovica Simoncelli

Matricola n. 623502

CORRELATORE

Chiar.mo Prof. Alessandro Orsini

ANNO ACCADEMICO 2014 – 2015

Indice

Introduzione

I crimini informatici sono fenomeni in continua crescita[1]; ciò in ragione del fatto che il rischio associato alla commissione del reato è basso se paragonato agli alti guadagni che ne derivano. Per questa ragione le informazioni trasmesse online sono considerate alla stregua di materie prime essenziali per il funzionamento di una nazione e il suo successo nell'area internazionale[2]; si tratta di "un complesso di informazioni su progetti, brevetti, piani strategici e quant'altro messo in una Rete che, anche se garantita dal muri digitali di protezione è, a quanto sembra, ancora troppo vulnerabile. Infatti, a rischiare attacchi cibernetici sono proprio i paesi a maggior dotazione di *know how*, innovativo e con alta esposizione in Rete. È la doppia faccia di Internet e dei vantaggi che offre l'innovazione dei sistemi ICT […]"[3].

Il pericolo maggiore degli attacchi cibernetici è costituito forse dalle due caratteristiche principali di questa tipologia di attacchi. La prima di esse è la cd. asimmetria degli attacchi, ossia la possibilità per chi colpisce di farlo in maniera assolutamente anonima, rapidissima e ad una grande distanza rispetto al dispositivo attaccato, poiché, spesso, è necessaria la presenza di una rete Internet; la seconda caratteristica invece è costituita dalla potenziale semplicità degli attacchi, che sono diventati soprattutto negli ultimi anni accessibili anche ad individui non dotati di particolari capacità tecniche.[4]

---

[1] *Rapporto Clusit 2015 sulla sicurezza ICT in Italia*, p. 100.

[2] FALLETTA P., MENSI M., *Il diritto del Web. Casi e materiali*, Padova, CEDAM, 2015, pp. 292-293.

[3] TAPPERO MERLO G., *Soggetti e ambiti della minaccia cibernetica: dal sistema paese alle proposte di cyber governance?* in *La Comunità Internazionale*, Fasc. 1/2012, pp. 25-53.

[4] Presidenza del Consiglio dei Ministri, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, 2013, p. 11.

Per queste ragioni la difesa dello spazio cibernetico diventa ogni giorno più essenziale per prevenire i rischi di attacco e garantire una sicurezza che ogni giorno di più si dimostra fondamentale per i singoli Paesi. L'*International Telecommunication Union* (ITU) delle Nazioni Unite definisce la *cybersecurity* come "l'insieme di strumenti, interventi, concetti, linee guida, impostazioni della gestione del rischio, azioni pratiche, procedute e tecnologie che possono essere utilizzate per proteggere lo spazio e la struttura cibernetica e i loro utilizzatori"[5]. In altri termini, la *cybersecurity* è considerata il contesto in cui cercare soluzioni ed elaborare strategie combinate al fine di difendere lo spazio cibernetico dalle minacce sia a livello nazionale sia transnazionale, dato il carattere spiccatamente globale della minaccia.[6]

Oggetto dello studio è la ricognizione delle tipologie di crimini informatici nate nel corso degli anni all'interno della quale si prevede di analizzare le risposte normative a questi reati, sia dal punto di vista dell'ordinamento interno che da quello della cooperazione internazionale, attraverso l'esame della disciplina del legislatore e delle istituzioni sovranazionali.

Nel primo capitolo sarà affrontata la tematica dei reati informatici attraverso una loro definizione più specifica che permetta di comprendere i diversi criteri di classificazione utilizzati dalla dottrina e dalla giurisprudenza al fine di suddividerli in ambiti tematici. In questa sezione inoltre verranno analizzati alcuni dei più frequenti illeciti informatici per comprenderne meglio le modalità di azione e le tipologie di abuso che compiono all'interno dei sistemi informatici.

Nel secondo capitolo si procederà invece con l'analisi della normativa italiana in merito ai crimini informatici, dando rilievo agli articoli introdotti o modificati dalla l. n. 547/1993 che rappresenta la prima normativa strettamente relativa alla disciplina dei reati informatici. Verranno evidenziate le differenti

---

[5] UN ITU, *Overview of Cybersecurity. Recommendation* UTI-T X.1205, Ginevra, UN, 2008.

[6] FALLETTA P., MENSI M., *supra* nota 2, p. 294.

posizioni della dottrina e della giurisprudenza in merito all'interpretazione delle varie disposizioni e saranno operate delle riflessioni in merito all'appropriatezza delle scelte di disciplina di determinate condotte da parte del legislatore.

Il terzo capito invece interesserà il contesto europeo e la cooperazione transnazionale, dal momento che l'ambito di azione dei *cybercrimes* interessa il più delle volte diversi Paesi contemporaneamente. Saranno analizzati gli atti più importanti per l'evoluzione e la creazione di strumenti di difesa da parte delle istituzioni europee: un ruolo centrale verrà riservato alla Convenzione del Consiglio d'Europa in materia di *Cybercrime*, il primo atto che dispone una serie di norme pattizie a cui debbano ottemperare gli Stati membri che hanno ratificato il documento. Si tratterà inoltre del recepimento della Convenzione di Budapest in Italia, avvenuto attraverso la l. n. 48/2008 di ratifica, che ha apportato alcune significative modifiche al c.p. e al c.p.p., sebbene anche in questo caso ci siano stati pareri discordanti in merito agli ambiti di applicazione della norma. Saranno infine prese in considerazione le disposizioni successiva alla Convenzione di Budapest, incentrate in modo particolare sulla creazione di un dialogo costante fra gli Stati al fine di armonizzare le normative e gli strumenti di disciplina degli illeciti nel c*yberspazio*.

Capitolo I

Gli illeciti nel Cyberspace

1. Definizione di crimine informatico

Il primo pensiero che soggiunge nel momento in cui si parla di reati informatici è che si tratti di un argomento piuttosto recente, e di conseguenza recentemente disciplinato. Sorprende invece scoprire che la legge a cui si fa riferimento *in primis* nel caso dei crimini informatici è la l. n. 547/1993, una legge che quindi ha 23 anni ma che ancora risulta fumosa nei suoi contenuti: infatti, a tutt'oggi risulta a volte difficile comprendere su quali reati volesse andare ad agire il legislatore. Infatti, la l. n. 547/1993 ha introdotto alcune disposizioni volte ad incriminare i reati informatici[7] ed alcune di esse sono state successivamente modificate a seguito della ratifica italiana alla Convenzione di Budapest sul *Cybercrime* (23 Novembre 2001), attraverso la l. n. 48/2008.

---

[7] La l. n. 547/1993 ha aggiunto nuove disposizioni e ne ha modificate altre per rimanere al passo con l'evoluzione delle tecnologie informatiche.
Le fattispecie inserite ex novo sono: art. 491-*bis* (Falso informatico); art. 615-*ter* (Accesso abusivo ad un sistema informatico o telematico); art. 615-*quater* (Detenzione e diffusione abusiva di codici d'accesso ad un sistema informatico o telematico); art. 615-*quinquies* (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico); art. 617-*quater* (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche); art. 617-*quinquies* (Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche); art. 617-*sexies* (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche); art. 623-*bis* (Rivelazione di comunicazioni telematiche); art. 635-*bis* (Danneggiamento di sistemi informatici e telematici); art. 640-*ter* (Frode informatica).
Le fattispecie preesistenti, modificate dalla l. n. 547/1993 comprendono invece: art. 392 (Esercizio arbitrario elle proprie ragioni mediante danneggiamento informatico); art. 420 (Attentato a sistemi elettronici di pubblica utilità); art. 616 (Violazione di corrispondenza telematica); art. 621 (Rivelazione del contenuto di documenti segreti su supporti informatici).

Diventa necessario dunque acquisire una maggiore consapevolezza in merito ai rischi che si corrono nel momento in cui si decide di utilizzare i sistemi informatici e le nuove tecnologie che fanno oggi parte della nostra quotidianità in ogni ambito, dall'economia alla pubblica amministrazione ma anche semplicemente nella vita privata degli individui, che spesso sono all'oscuro dei pericoli che si nascondono specialmente all'interno della rete. È fondamentale comprendere il corretto funzionamento di tali tecnologie, i rischi che si corrono e le potenziali condotte illegali realizzabili con esse.

I reati informatici sono convenzionalmente denominati *cybercrimes* poiché presentano come elemento comune l'uso di dispositivi elettronici. L'influenza della cd. *information technology* sulla commissione e percezione dell'illecito non è spiegabile attraverso i tradizionali canoni e approcci delle scienze criminologiche. Tuttavia, definire in modo puntuale i *cybercrimes* non è semplice poiché questo termine include al proprio interno una serie di condotte illecite molto diverse fra loro, di varia natura, tutte unite dal denominatore comune che è l'utilizzo di un computer o di un dispositivo informatico.

Parte della dottrina distingue fra *computer fraud* e *computer abused*[8]. Le *computer fraud* comprendono al proprio interno tutti i comportamenti manipolativi con scopi fraudolenti, mentre le *computer abused* integrano tutte le condotte che prevedono degli usi impropri delle tecnologie al fine di ottenere vantaggi. Altri suddividono i crimini informatici in crimini propriamente informatici ed eventualmente informatici[9], in base all'essenzialità del ruolo del dispositivo nella condotta; i reati propriamente informatici non sussistono in assenza di strumenti informatici o telematici, mentre i reati informatici in senso lato comprendono le fattispecie penalmente rilevanti consumabili anche al di fuori dello spazio cibernetico.

---

[8] PARKER D.B., *Cryme by Computer*, New York, Charles Scribsen's Sons, 1976; CREMONI C., MARTELLA G., *I crimini informatici: storia, tecniche e difese*, Milano, Mondadori, 1990, p. 40.

[9] BORRUSO V.R., in BORRUSO V.R., BUONOMO G., CORASANITI G., D'AIETTI G., *Profili penali dell'informatica*, Milano, Mondadori, 1994, pp. 4 ss.

Sebbene parte della dottrina abbia ricondotto tutti i crimini informatici sotto l'alveo di *computer crimes*[10], quindi, tale classificazione così generica risulta poco idonea a comprendere il fenomeno in tutti i suoi aspetti eterogenei, dando un'immagine falsata dell'ampiezza del mondo dei crimini informatici. I comportamenti criminali così definiti hanno in comune una serie di caratteristiche, come ad esempio il superamento dei confini spazio temporali, che rendono necessario un approccio casistico e non una distinzione dei reati per macrocategorie[11].

I problemi legati all'utilizzo illegale dei nuovi strumenti delle tecnologie cominciano a manifestarsi in maniera evidente a partire dagli anni Ottanta, con l'introduzione del personal computer e l'utilizzo delle tecnologie informatiche da parte delle masse; precedentemente infatti l'utilizzo delle tecnologie elettroniche era riservato a istituzioni accademiche e basi militari[12].

Negli anni Ottanta, oltre alla massificazione dell'utilizzo delle tecnologie, si sviluppa anche la cultura dell'*hacking* fra i giovani: è riassumibile nell'idea che le informazioni contenuta nei computer debbano essere condivise da tutti, anche se questo significa l'accesso a dispositivi altrui senza precedente consenso da parte dei proprietari.

Inoltre, i mezzi elettronici cominciano a sostituire i tradizionali documenti cartacei, e la "rivoluzione digitale" si accompagna ad una "rivoluzione criminale", poiché le nuove tecnologie informatiche si rivelano terreno fertile

---

[10] VACIAGO G., *Internet e i crimini informatici*, in PICCINI M.L., VACIAGO G., *Computer crime: casi pratici e metodologie investigative dei reati informatici*, Bergamo, Moretti&Vitali, 2008, pp. 12 ss.

[11] IASELLI M., MAGGIOPINTO A. (a cura di), *Sicurezza e anonimato in Rete. Profili giuridici e tecnologici della navigazione anonima*, Milano, Nyberg, 2005, pp. 16 ss.

[12] Per approfondire le fasi dell'evoluzione della criminalità informatica, cfr. CLOUGH J., *Principles of cybercime. Part I-III*, Cambridge, Academic Press, 2010, pp. 3-67

in cui nuove espressioni del crimine organizzato occupano uno spazio direttamente proporzionale al sempre maggiore utilizzo dei dispositivi[13].

Il reale punto di svolta avviene però negli anni Novanta con l'avvento di Internet: questo strumento risulta parte integrante della quotidianità, elemento insostituibile nella vita economica, culturale e sociale di tutto il mondo occidentale[14], ha dato il via alla creazione di una serie di illeciti che utilizzano il Web per modernizzarsi e moltiplicarsi. Internet costituisce il nido di due tipologie diverse di reati ed illeciti: da una parte, quelli "tradizionali", che esistevano a prescindere dalla tecnologia online ma che utilizzano la rete come nuovo strumento per realizzarsi; dall'altra quelli che invece non trovano una vera e propria corrispondenza con il mondo "fisico" e che pertanto costituiscono dei veri e propri reati nuovi, che hanno pertanto bisogno di leggi *ad hoc*. Ad esempio, si prenda il caso del furto d'identità digitale sul web: il reato in questione non è assimilabile al furto tradizionale, né tantomeno al trattamento abusivo di dati personali. A volte però mancano tali disposizioni *ad hoc*, pertanto dottrina e giurisprudenza cercano di uniformarsi per riempire le lacune giuridiche in merito[15].

2. Elementi che definiscono la sicurezza in Rete

La continua crescita della Rete e dei sistemi di informazione nella vita quotidiana in tutti suoi aspetti, pone il problema fondamentale il fattore sicurezza. Genericamente, possiamo definire la sicurezza delle reti e dell'informazione come la capacità di esse di resistere ad armi dolosi o eventi imprevisti che

---

[13] LORUSSO P., *L'insicurezza dell'era digitale. Tra cybercrimes e nuove frontiere dell'investigazione: Tra cybercrimes e nuove frontiere dell'investigazione*, Milano, Franco Angeli, 2011, p. 15.

[14] Per l'esame del *Digital Divide* negli anni Novanta con l'avvento di Internet, si rimanda a NORRIS P., *The Worldwide Digital Divide: Information Poverty, the Internet and Development*, Cambridge, John F. Kennedy School of Government Harvard University, 2000, p. 3.

[15] BETZU M., *Regolare Internet. La libertà di informazione e di comunicazione nell'era digitale*, Torino, G. Giappichelli Editore, 2012, pp. 81 s.

possono compromettere i quattro elementi essenziali, ossia la disponibilità, l'autenticazione, l'integrità e la riservatezza dei dati, dei servizi forniti o accessibili attraverso la rete stessa[16]. La *disponibilità* è l'effettiva accessibilità dei dati e dei servizi anche in caso di interruzioni dovute ad eventi imprevisti o ad attacchi di pirateria informatica; l'*autenticazione* è la conferma dell'identità dichiarata da un organismo o un utente, anche se in alcuni casi è necessario comprendere la possibilità del mantenimento dell'anonimato, quando non è necessaria la conoscenza del profilo anagrafico dell'utente; l'*integrità* è il mantenimento dei dati trasmessi esattamente come sono, senza tagli o modifiche; la *riservatezza*, infine, è orientata alla protezione dei dati e risulta importante nel caso di trasferimento di dati sensibili che fanno parte delle informazioni relative alla vita privata degli utenti.

3. Reati informatici e reati connessi a sistemi informatici: un confronto

Il reato informatico è un reato che per essere commesso con successo necessita della conoscenza del funzionamento del computer, mentre in un reato connesso all'informatica il computer è usato solo come mezzo ad obiettivo di reato, indipendentemente dalla conoscenza che si ha sul funzionamento della macchina[17].

---

[16] Commissione Europea, *Una strategia per una società dell'informazione sicura - Dialogo, partenariato e responsabilizzazione,* COM(2006) 256, Bruxelles, 3.

[17] "White collar crimes cover many acts that may, but need not, include the use of a computer as an essential element of the crime. Examples are antitrust violations, public corruption, bribes, environmental pollution, and price fixing. Computer crimes can also include white collar crimes but need not be limited to those types of acts. Examples of non-white collar crimes are virus attacks on computer systems, as well as acts of violence or unauthorized changes in computers that control industrial processes." cfr. PARKER D., *Computer Crime: Criminal Justice. Resource Manual,* National Institute of Justice, U.S. Department of Justice, 1989, p. 7.

Pertanto, nel caso dei reati informatici si manifesta la necessità di un vero e proprio aggiornamento dei codici penali internazionali ai fini di comprendere questi nuovi illeciti per poterli disciplinare, mentre nel caso dei reati connessi all'informatica, che non sono quindi altro che reati tradizionali che utilizzano il mezzo informatico, c'è necessità di una cooperazione e della creazione di misure procedurali più aggiornate, complete e quindi migliori.

Tali modifiche dei codici penali affrontano una serie specifica di reati, e nello specifico quattro tipologie che verranno qui analizzate:

- *Reati contro la riservatezza*, i quali sono relativi agli illeciti che concernono la raccolta, la memorizzazione, l'alterazione, la divulgazione e la diffusione di dati personali; in merito è fondamentale citare la direttiva 58/2002 CE del Parlamento Europeo e del Consiglio del 12 Luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, che prende come modello principale la direttiva 95/46 CE, a sua volta relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

- *Reati relativi ai contenuti*, ossia quei reati relativi alla diffusione, della pornografia e della pedopornografia, di affermazioni razziste e di informazioni che incitino alla violenza; il dubbio che ci si è posti è quanto il diritto penale tradizionale possa costituire una fonte autorevole per la disciplina di tali illeciti ed in merito la Commissione ha sostenuto la tesi che ciò che risulta illecito off-line deve essere tale anche on-line; la direttiva 2000/31 CE sul commercio elettronico stabilisce la responsabilità dei fornitori di servizi che agiscono come intermediari in rete.

- *Reati contro il patrimonio, accesso non autorizzato e sabotaggio*, che spesso definiscono nuove fattispecie di reati strettamente connessi all'elemento "elettronico" dell'illecito, legate appunto all'accesso non autorizzato ai sistemi informatici e nuove modalità di violazione.

- *Reati contro la proprietà intellettuale,* in merito alle quali il Consiglio ha adottato due direttive, una del 2005 e l'altra nel 2006, trattanti tematiche

strettamente connesse alla società della comunicazione e dell'informazione elettroniche e prevedono l'adozione di sanzioni *ad hoc* per tutelare specialmente le banche dati.

4. La figura dell'hacker le metodologie di accesso abusivo

La premessa da cui spesso si parte nel momento in cui si prendono in considerazione le modalità di intrusione nei sistemi informatici, è che sia necessaria una avanzatissima abilità tecnica. Tale premessa è sbagliata e frutto di una sostanziale inconsapevolezza. Infatti, ci sono svariate modalità per inserirsi all'interno delle reti informatiche; spesso è sufficiente scaricare un programma automatico da Internet per poter effettuare anche le più complesse manipolazioni sui dispositivi pur non avendo capacità informatiche o conoscenze tecniche superiori alla media.

Il primo elemento da chiarire è la definizione del concetto di *hacking:* un comportamento il cui scopo è quello di violare la sicurezza dei sistemi informatici e delle reti telematiche. Lo scopo di lucro non è necessariamente la ragione principale che muove gli *hacker*, molto spesso si tratta soprattutto di finalità puramente ludiche; tuttavia, è frequente che dal passatempo si passi allo sfruttamento dei dati raggiunti e all'inserimento di programmi dannosi all'interno del sistema.[18]

[18] Il termine *hacker* è in realtà troppo generico, poiché raggruppa al proprio interno varie tipologie di soggetti che operano in maniera molto differente fra loro e che vengono classificati in base ai propri intenti e alle conseguenze delle proprie azioni. Gli hacker si suddividono infatti in *white hat hacker* (gli hacker dal cappello bianco), il cui intento principale è quello di riparare i danni e le falle nella sicurezza, e in *black hat hacker* (gli *hacker* dal cappello nero), che sono invece quelli che creano i danni. Ci sono poi i *grey hat hacker* (gli *hacker* dal cappello grigio), i quali si collocano in una zona intermedia e che sono la prova del fatto che il confine fra una buona azione e un illecito online è piuttosto labile, perché non sempre l'intenzione positiva corrisponde ad un'azione legale. Il termine hacker è quindi utilizzato in accezione ampia, dal momento che in gergo tecnico gli "*hacker* dal cappello nero" vengono più spesso denominati *cracker*. MOORE R., *Cybercrime: investigative high-technology computer crime*, LexisNexis Publication, 2005, p. 24 s.; SALVADORI I., *Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive* de iure condendo, in *Ciber. Dir.*, 2008, n. 9. p. 344.

Ci sono moltissimi metodi che permettono l'intrusione nei sistemi informatici di varia difficoltà e tipologia: da quelli più semplici e rudimentali a quelli che necessitano di maggiori capacità e tecnologie più avanzate, da quelli che permettono un'azione a distanza a quelli più immediati che prevedono la violazione *in loco*, specialmente nel caso di intrusioni nei sistemi aziendali.

In questo caso, ad esempio, è necessario che l'autore dell'illecito sfrutti le proprie credenziali di accesso al sistema o quelle di un collega, o se la procuri attraverso varie tecniche estremamente banali ma sufficientemente efficaci. La prima è il cd. *should surfing*[19], che può essere semplicemente tradotta in "sbirciata di spalle", perché si tratta di spiare il titolare di un codice di accesso (alle spalle dell'individuo) nel momento in cui immette il codice stesso e tenerlo a mente per utilizzarlo successivamente; tra l'altro, per il furto di carte di credito o conti bancari è il metodo più semplice ed efficace.

Un metodo già più complesso è costituito dai meccanismi di *social engineering*, la cd. "ingegneria sociale". Il nome potrebbe far pensare a qualcosa di matematico o scientifico, ma è ingannevole: infatti, si tratta di sfruttare piuttosto la psicologia della vittima ai fini di persuaderla a fornire le proprie credenziali di accesso al sistema. Questo implica un comportamento di base ingannevole da parte dell'*hacker*, il quale si finge qualcun altro, magari al telefono con le vittime, riuscendo spessissimo a convincerle. Le vittime inconsciamente sono portate a cedere con facilità le informazioni richieste, senza richiedere ulteriori verifiche o prove dell'identità del soggetto che le sta richiedendo[20]. Questa stessa attività illecita ha il suo corrispettivo online, denominato *phishing,* caso in cui la falsa identità dell'autore dell'illecito si manifesta tramite l'utilizzo di e-mail e non telefonicamente ma che presenta comunque le stesse caratteristiche e richieste dell'ingegneria sociale. Il fenomeno del *phishing*,

---

[19] CLIFFORD R.D. (ed.), *Cybercrime: the investigation, prosecution and defense of a computer-related crime*, Durham, Carolina Academic Press, 2011, p. 193.

[20] L'inventore di questo metodo, come di quello dello *spoofing*, di cui parleremo, può essere considerato "Condor", al secolo Kevin Mitnick, del quale si parla in MOORE R., *Cybercrime: investigative high-technology computer crime,* cit., p. 62 s.

però, è totalmente altro rispetto al fenomeno dell'*hacking*, in quanto l'autore dell'illecito non soltanto accede al sistema informatico della vittima, ma ne sfrutta anche il profilo finanziario; questa differenza ha delle importanti conseguenze dal punto di vista giuridico, in quanto mentre l'*hacking* si colloca all'interno delle fattispecie regolate dall'art. 615 *ter* c.p., il *phishing* è qualificabile come truffa nel momento in cui il *phisher* consegua successivamente un'utilità patrimoniale, e pertanto riconducibile all'art. 640 c.p.[21]

Un metodo più complesso è quello che considera l'esistenza e l'installazione di programmi di *key-logging*[22]: tali programmi registrano e inviano al computer connesso ogni tasto premuto sulla tastiera del computer della vittima, in modo tale che l'*hacker* ottenga immediatamente la password non appena la vittima la digita. Questa tecnologia è spesso utilizzata con scopi non illegali, ma piuttosto per individuare altri crimini informatici da parte dei corpi di polizia tecnologicamente avanzati come ad esempio l'FBI, che utilizza la tecnica che *key-logging* per effettuare intercettazioni telematiche, pur talvolta rischiando di oltrepassare il limite (che rimane sempre piuttosto labile) della riservatezza degli indagati[23].

Un'altra tipologia di azione illegale in rete che permette facilmente all'hacker di attaccare un sistema è quella che utilizza i cd. *decryptor*, software di decifrazione di password che però risulta estremamente complesso e costoso e pertanto utilizzato soltanto in grandi operazioni di violazione dei sistemi.

Al contrario, maggiormente utilizzato è il meccanismo di cifratura, che consente all'autore dell'azione illegale di nascondere il procedimento attraverso cui è riuscito a scoprire la password impedendo così una qualsiasi indagine a suo danno.

---

[21] L'argomento sarà trattato in dettaglio nel Capitolo II.

[22] SMITH R.G., GRABOSKY P., URBAS G., *Cyber criminals on trial*, su *key-loggers*, *decryptors* e utilizzo investigativo dei meccanismi di hacking da parte della polizia USA, Cambridge University Press, 2004. p. 305 s.

[23] Esempi di tale condotta dell'FBI: cfr. CLOUGH J., *Principles of Cybercrime*, Cambridge University Press, 2015, pp. 164 ss.

Altre modalità di inserimento nei sistemi informatici di inconsapevoli vittime sfruttano l'inserimento di comandi dannosi all'interno di siti "puliti", in modo tale che nel momento dell'inserimento dei dati, l'*hacker* possa ottenere direttamente queste informazioni e possa anche risalire alla loro fonte, collegandosi alla cronologia e ai movimenti connessi al computer "base".

Questi sono solo alcuni dei metodi di inserimento nei sistemi informatici da parte degli *hacker* che sfruttano tecnologie più o meno complesse e costose e che pertanto possono essere messi in atto da professionisti ma anche da dilettanti alle prime armi.

5. Strumenti di commissione dei reati informatici

I casi di inserimento di programmi dannosi all'interno di sistemi informatici sono quelli più temuti dagli utenti che utilizzano tecnologie informatiche e navigano in rete[24]. Questo probabilmente perché la diffusione di tali programmi sta crescendo in maniera esponenziale, rappresentando quindi una grande minaccia alla sicurezza delle reti e delle informazioni. Per procedere con l'esame degli aspetti penali relativi al danneggiamento di un sistema informatico a causa dell'immissione di programmi dannosi è fondamentale comprendere almeno in grandi linee come si suddividono tali programmi e quali danni causano.

In gergo informatico, i programmi atti a causare danni all'interno dei sistemi sono definiti *malware*, crasi di *malicious software*, ossia software maligni che provocano malfunzionamenti dei sistemi e delle reti[25]. I *malware* sono suddivisibili genericamente in quattro grandi categorie, che possono sussistere

[24] Dati Symantec, reperibili nell'*Internet Security Threat Report* 2010 (Relazione sui rischi per la sicurezza in Internet).

[25] SALVADORI I., *Hacking, cracking e nuove forme di attacco ai sistemi d'informazione. Profili di diritto penale e prospettive de iure condendo*, in *Ciber. Dir.*, 2008, n. 9, p. 348.

singolarmente oppure interagire fra loro, come fossero elementi di un unico grande programma: esistono i *virus*, i *worm*, i *trojan horse* e le *backdoor*, ognuno dei quali ha effetti ed entità di danno diversi.

I *virus* sono i *malware* più conosciuti dagli utenti, nonché la categoria più vasta e diffusa in rete; per questa ragione, spesso si utilizza il loro nome con significato improprio, considerando *virus* tutte le tipologie di malware. Tuttavia, con questo termine si intende definire solo l'insieme di programmi dannosi che sono ospitati all'interno di un altro programma apparentemente innocuo, attraverso il quale si diffondono nei sistemi. Il meccanismo di attivazione del *virus* può avvenire nel momento in cui il programma che lo contiene si attiva, oppure dopo un periodo di tempo prestabilito (il caso delle cd. *logic bomb*)[26]. Per progettare un *virus* è necessario semplicemente acquistare il programma online, un vero e proprio "*virus kit*" che guida l'utente attraverso una vera e propria creazione dei virus, a seconda delle esigenze richieste da chi acquista il pacchetto; la diffusione poi è di semplicissima esecuzione, poiché si utilizza la rete internet che raggiunge moltissimi dispositivi in brevissimo tempo.

Tuttavia, il tipo di *malware* più diffuso all'interno dei sistemi informatici sino dall'avvento della rete Internet è certamente quello dei *worm*, che si distinguono dai semplici *virus* grazie al loro carattere autosufficiente: infatti il *worm* è in grado di sopravvivere anche senza alcun programma che lo inglobi[27]. Questa tipologia di *malware* sfrutta i cd. *bugs* (errori o falle) dei sistemi, per inserirsi all'interno di essi e riprodursi: è proprio questo il principale obiettivo del *worm*, creare uno spiraglio per incrinare i sistemi di sicurezza di un dispositivo che solo eventualmente in un secondo momento potrà essere infettato da *virus* che porteranno alla cancellazione della memoria elettronica o

---

[26] ZICCARDI G., *I virus informatici: aspetti tecnici e giuridici, in Ciber. Dir.*, 2001, fasc. 3-4, p. 350 s.

[27] Bollettini di sicurezza rilasciati fino a Dicembre 2015 dal Microsoft Security Center; cfr. https://technet.microsoft.com/library/security/ms15-dec .

piuttosto a malfunzionamenti dei sistemi stessi; pertanto anche in questo l'azione differisce da quella dei *virus*.

Altro *malware* da considerare è il cosiddetto *trojan*, o Cavallo di troia, che si presenta come un programma inoffensivo accettato dal destinatario in ragione dell'apparente mittente o del contenuto ostentato[28]. I *trojan* hanno come caratteristica fondamentale la necessità di essere attivati attraverso un'azione da parte della vittima, e quindi si inseriscono all'interno di programmi che prevedono che gli utenti agiscano in qualche modo; l'alternativa, è che il *trojan* si trasmetta attraverso un *worm*, agendo in maniera congiunta[29]. Il *trojan* permette all'*hacker* di poter agire direttamente sul sistema del dispositivo infetto e compiere operazioni sulle informazioni contenute in esso perché sottrae il dominio del dispositivo al legittimo proprietario senza che esso se ne accorga. Questo meccanismo porta sia alla possibilità di furti di informazioni che anche alla possibilità di controllo remoto del dispositivo per potenziali attacchi informatici. Per questa ragione spesso il *trojan* non agisce nel momento stesso in cui viene rilasciato nel dispositivo infetto, ma si risveglia dopo un periodo di inattività creando dei sistemi "*zombie*" che essendo stati violati agiscono solo in funzione dei comandi dell'*hacker* stesso, dando vita al cd. fenomeno dei *botnet,* ossia la diffusione massiccia di programmi *trojan*[30].

L'ultimo dei quattro principali *malware* presenti nei sistemi informatici è quello delle *backdoor*, letteralmente "porta sul retro", un'entrata di servizio segreta agli occhi di tutti meno che a quelli dell'*hacker*, il quale può entrare indisturbato all'interno del sistema. In questo modo, chi si inserisce e prende possesso del dispositivo, soprattutto facendolo da remoto, ha a disposizione un

---

[28] AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Matelica, Halley Editrice, 2006, p. 177.

[29] SARZANA DI S., IPPOLITO C., *Informatica, Internet e diritto penale*, Milano, Giuffré Editore, II ed., 2003, pp. 44-47.

[30] CASEY E., *Digital evidence and computer crime. Forensic Science, Computers and the Internet*, Cambridge Mass., Academic Press, p. 70 s.

raggio vastissimo di azioni che può compiere danneggiando la vittima, ossia il proprietario del dispositivo[31].

A differenza dei *malware*, i sabotaggi informatici sono forme di abuso che causano per loro stessa definizione il *crash*, la paralisi dei sistemi operativi attaccati; vengono chiamati in gergo *DoS*, acronimo che sta per *Denial of Service* (blocco del servizio), e a volte hanno alla base motivazioni relative ad ideologie che prendono di mira enti, governi, imprese e siti web di pubblica utilità, come se si trattasse di una forma di protesta o mobilitazione virtuale. Più recente è la creazione dei cosiddetti *DDoS*, ossia *Distributed Denial of Service*, che utilizzano computer già precedentemente infettati da *trojan* che quindi sono diventati veri e propri robot coordinati a formare una rete di *botnet*. In questo modo, chi effettua l'attacco ha a disposizione una sorta di esercito di computer-robot programmati precedentemente per agire come una bomba ad orologeria in maniera coordinata e congiunta. Un episodio emblematico si ritrova nel caso della diffusione del *worm Stuntnext*[32], rilasciato nel 2010 in Estonia; questo attacco causò un fortissimo shock all'UE e agli esperti in sicurezza informatica, in quanto era stato attaccato un paese che veniva tendenzialmente preso ad esempio per l'alto livello di sicurezza informatica. Caratteristica di questo tipo di sabotaggio, anche e soprattutto nel caso appena citato, è che gli autori di esso rimangano ignoti per molto tempo, o anche per sempre, dopo l'attacco: nel caso di *Stuntnext*, ad esempio, sono state formulate numerose ipotesi, non ultima quella che prende in considerazione l'azione compiuta da USA e Iraq ai danni dell'Iran, paese del quale figuravano numerosi computer delle centrali nucleari affetti dal *worm*[33].

Altre forme di sabotaggio sono ad esempio il *defacing* e il *netstrike*. Il *defacing* consiste nel cambiare in qualche modo l'aspetto di una pagina web

---

[31] Cfr. *Osservatorio sulla criminalità informatica*, Milano, Franco Angeli, 1997, p. 51.

[32] Reportage consultabile al sito http://www.wired.com/politics/security/magazine/15-09/ff_estonia .

[33] http://uk.reuters.com/article/2010/09/24/us-security-cyber-iran-fb-idUKTRE68N3PT20100924

ed è un meccanismo utilizzato soprattutto in segno di protesta, magari con la pubblicazione online di messaggi offensivi o di mobilitazione o addirittura una schermata nera nei casi più estremi e forti[34]. Il *netstrike*, invece, può essere assimilato ad una sorta di *DoS* nel meccanismo, ma sono le intenzioni che muovono gli utenti ad agire che cambiano. Infatti, nel caso del *netstrike*, si può parlare di veri e propri scioperi virtuali che non causano danni permanenti ma sono solo volti a disabilitare temporaneamente l'accesso a siti nei confronti dei quali è in atto una forma di protesta. Non si tratta quindi di un vero e proprio sabotaggio, perché è più inquadrabile come una sorta di disobbedienza momentanea dei cosiddetti *hacktivist* (crasi di *hacker* e *activist*), anche se tuttavia il confine fra le due tipologie di danno è molto labile e ci sono molti casi in cui episodi di *netstrike* hanno completamente impedito le comunicazioni con il sito attaccato e sono stati quindi inquadrabili all'interno de reato disciplinato all'art. 617-*quater* c.p.[35].

6. Illeciti "eventualmente" informatici

Saranno ora analizzati i casi degli illeciti che rientrano nella categoria dei reati informatici nel linguaggio comune, ma che non sono considerabili propriamente tali a causa delle loro caratteristiche intrinseche. Infatti, gli illeciti sopra descritti hanno come carattere necessario l'esistenza del mezzo tecnologico, poiché sono nati con esso: nel momento in cui non sussiste la presenza dell'oggetto, il reato non può verificarsi. L'esempio emblematico è quello della diffusione di un *malware*, che chiaramente non si verifica nel momento in cui non esiste il computer da cui farlo partire; il reato interessa il *software*, che è inquadrabile come un contenitore di informazioni che tuttavia è immateriale,

[34] CLOUGH J., *Principles of cybercrime*, Cambridge, 2010, p. 38.

[35] L'art. 617-*quater* disciplina, *inter alia*, il reato di impedimento di comunicazioni intercorrenti fra più sistemi informatici.

una nuova tecnologia che non è tutelata in nessuna norma e che pertanto necessita di un provvedimento ad hoc per disciplinarne gli illeciti.

I reati di cui ci accingiamo a trattare, invece, sono quelli che esistono a prescindere dalla natura tecnologica del mezzo e delle informazioni che vengono violate, rendendo solo eventuale la presenza delle tecnologie, ma configurandosi piuttosto come condotte illecite anche senza l'ausilio di un computer o di informazioni necessariamente presenti in un *software*[36]. L'esempio più significativo è quello delle frodi e delle truffe informatiche, che in questo caso avvengono attraverso l'ausilio di Internet ma che si manifestano anche in altri modi che non necessariamente tengono in considerazione l'utilizzo di dispositivi tecnologici.

Tuttavia, nella pratica risulta sempre più complesso dividere i reati secondo una classificazione così schematica, in quanto sono moltissimi i casi in cui la sovrapposizione dei reati non permette una chiara comprensione di quanto sia necessaria la sussistenza del *software* e del mezzo tecnologico per l'esecuzione dell'illecito[37]. Il concetto di reato informatico proprio o improprio, quindi, tende a variare essendo il confine molto difficile da stabilire.

Il primo caso che andiamo ad analizzare è quello delle intercettazioni telematiche, presente sulla scena degli illeciti informatici già a partire dagli anni Sessanta: in quegli anni venivano sfruttate le falle nella sicurezza delle reti telefoniche per dirottare le comunicazioni a insaputa della vittima e spostare la comunicazione su reti interurbane, intercontinentali o comunque a tariffazione maggiorata. Per fare ciò, gli hacker del tempo, chiamati *phreaker* (crasi di *phone* e *hacker*) sfruttavano la cd. "scatola di disturbo", la *blue box,* che smistava le telefonate. Oggi la *blue box* non è più utilizzata, ma al suo po-

---

[36] Ci si rifà alla dottrina anglosassone, vedi RICHARDS J., *Transnational criminal organizations, Cybercrime and money laundering*, New York, CRC, 1999, p. 63; ma anche continentale, SIEBER U., *The international handbook for computer crime. Computer-Related Economic Crime and the Infringements of Privacy*, New York, Wiley, 1986, p. 12.

[37] ALMA M. - PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Dir. Pen. Proc.*, 1997, pp. 506-507.

sto esiste il *dialer*, programma vendibile online dai Service Provider e scaricabile direttamente sul proprio dispositivo, che crea un collegamento con il Web, nello specifico con servizi a tariffe superiori nel momento in cui l'utente apre la pagina web; infatti in quel momento la consueta connessione Internet si disabilita, in favore un'altra più costosa[38]. Questo supporto è stato inventato principalmente con fini leciti, e in questo caso l'utente che decide di scaricare il programma lo fa volontariamente, lo attiva quando preferisce e ha continuamente la possibilità di disabilitarlo tornando alla connessione standard. Nel momento in cui, invece, viene utilizzato con fini illeciti, la vittima scarica il programma in maniera inconsapevole o molto spesso è il programma stesso ad inserirsi all'interno del dispositivo infetto grazie al supporto di un *worm* o un *virus*; inoltre, il *dialer* in questo caso opera da solo e si stabilisce una connessione privilegiata ininterrotta[39], quindi l'utente inconsapevole viene dirottato nelle sue comunicazioni verso un altro dispositivo o un numero telefonico interurbano o con tariffa maggiorata.

La realizzazione di questo tipo di intercettazioni, oggi, avviene anche semplicemente sfruttando le reti Internet, senza comprendere anche l'utilizzo di numeri di telefono, in maniera completamente telematica. Questo tipo di intercettazioni utilizza i programmi *spyware:* tali programmi consentono all'*hacker* di spiare le azioni dell'utente che si trova l'applicazione nel dispositivo, registrando anche le password digitate (il programma di cui parlavamo prima, *key-logger*, fa parte degli *spyware* più comuni). Dal momento in cui l'hacker ha accesso alle password della vittima, potrà intercettarne movimenti e comunicazioni.

È necessario però sottolineare un aspetto significativo: l'inserimento di uno *spyware* all'interno di un dispositivo giuridicamente non costituisce reato

---

[38] SIEBER U., *Organised crime in Europe: the threat of cybercrime. Situation Report 2004,* Strasburgo, Council of Europe Publishing, 2005, p. 126 s.

[39] SARZANA S., IPPOLITO C., *Informatica, Internet e Diritto Penale*, Milano, Giuffré, pp. 51-54.

di intercettazione di per se stesso, pur essendo il primo passo per la realizzazione delle intercettazioni vere e proprie. Per quanto riguarda l'immissione di uno *spyware* all'interno di un dispositivo, si può far riferimento all'art. 615-*ter* c.p., relativo all'accesso abusivo ad un sistema informatico.

Specificamente poi ci si deve soffermare sull'oggetto della condotta illecita, che è solo ed esclusivamente il contenuto dell'intercettazione, perché essa per configurare un reato deve attenersi alle comunicazioni in corso, esattamente come nel caso delle intercettazioni tradizionali. Tuttavia, non è così facile operare una netta distinzione fra comunicazioni archiviate ed attuali, a causa dei numerosi passaggi che si verificano nel momento in cui viene ad esempio trasmessa una email, passaggi durante i quali il messaggio viene temporaneamente archiviato una serie di volte[40]. Come devono essere considerate queste archiviazioni temporanee? A seconda che vengano considerate come effettive archiviazioni o come semplici "soste" del messaggio che comunque rimane in trasmissione, si configurano due diverse ipotesi di illecito, punibili rispettivamente secondo gli artt. 616 c.p. (violazione di corrispondenza) oppure 617-*quater* c.p. Tendenzialmente, l'orientamento giuridico pende verso la seconda ipotesi, in quanto l'archiviazione del messaggio è in questo caso temporanea e soprattutto propedeutica all'invio del messaggio all'utente finale, quindi qualificabile in tutto e per tutto come effettiva intercettazione telematica.

Anche il concetto di "contenuto" nella pratica diventa di difficile interpretazione, soprattutto nei casi in cui non si parli di intercettazione di messaggi di posta elettronica ma piuttosto di altre tipologie di contenuti, come ad esempio quelli scambiati in chat o magari sui *social network*. In questi casi, infatti, risulta difficile scindere il contenuto del messaggio dal suo contenitore,

---

[40] SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in *Riv. Trim. dir. Pen. Eco*, 1997, pp. 749-750.

ossia i dati relativi alla trasmissione del messaggio che però non costituiscono oggetto dell'illecito[41].

Un altro caso di illecito che rappresenta l'oggetto di controversie in merito alla definizione di crimine informatico è quello della falsificazione attraverso sistema informatico, che presenta contraddizioni di varia natura in merito all'oggetto dell'illecito: infatti è di difficile interpretazione se si debba considerare fattispecie penale il fatto che l'autore del documento non sia autentico oppure la veridicità del contenuto del documento. Secondo il DPR 10 Novembre 1997 n. 513 all'art. 11 "i contratti stipulati con strumenti informatici o per via telematica mediante l'uso della firma digitale secondo le disposizioni del presente regolamento sono validi e rilevanti a tutti gli effetti di legge". Tale definizione pone ancora maggiori preoccupazioni in merito al fenomeno delle false informazioni personali e al furto di identità digitale, poiché dimostra che ad oggi tutti i contratti possono essere stipulati online grazie all'utilizzo della firma digitale e pertanto risulta urgente e necessario chiarire i dubbi in merito al contenuto del codice penale.

Specificamente, il reato di falsificazione in scrittura privata informatica è previsto nel codice penale agli artt. 485 e 491-*bis*, che definiscono la fattispecie di reato e specificano sanzioni relative a documenti privati o pubblici. Nel dettaglio, l'art. 485 prevede il reato di colui che, "al fine di procurare a sé stesso o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera", mentre l'art. 495-*bis* oltre a definire le disposizioni previste per atti pubblici o privati, dà la definizione di documento informatico, intendendolo come qualsiasi supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati a elaborarli.

---

[41] PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. Pen. Eco.*, 1995, p. 419.

Questi due articoli ci permettono, dunque, di definire in maniera abbastanza chiara l'essenza della fattispecie penale di falso in scrittura privata informatica, che presenta sostanzialmente due caratteristiche principali: la volontà di procurare un vantaggio a se stessi o a terzi, e l'utilizzo della stessa "scrittura".

Tuttavia, le incertezze riguardano soprattutto la dicitura piuttosto ampia e generica del codice agli artt. 485 e 491-*bis*, poiché sembrerebbe che vengano incluse all'interno delle fattispecie di reato non soltanto la cd. firma digitale, ma anche ogni tipologia di sottoscrizione di contratti anche solo attraverso l'indicazione del proprio nome o delle proprie generalità; questo pone dei problemi di interpretazione perché va a sovrapporsi al reato disciplinato da un altro articolo del codice penale, il 615-*quater*, relativo alla detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici[42]. L'articolo definisce l'ipotesi di reato di colui che, "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". Alla base di questo comportamento abusivo vi è il furto di un'identità o la costituzione di un falso informatico, attività che rendono possibile il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici.

Ulteriori dubbi interpretativi sono rappresentati, inoltre, dalla possibile qualificazione del reato di falso informatico e furto dell'identità digitale come reati informatico proprio e improprio: se infatti è possibile ritrovare l'oggetto del reato nei dati informatici di un soggetto è anche vero che il reato è comunque identificabile come una violazione della privacy della vittima, avvenuta soltanto per mezzo di un qualche tipo di tecnologia, ma che potenzialmente

[42] Nel capitolo secondo sarà affrontata in maniera dettagliata l'analisi dell'articolo 615-*quater* c.p.

sarebbe potuta avvenire anche attraverso altri mezzi. In questo secondo caso, non ci sarebbe da riferirsi agli articoli del Codice Penale, ma piuttosto al Codice della Privacy, del quale si potrebbe in questo caso applicare la disciplina in senso estensivo e ampio[43].

Il caso delle frodi elettroniche è un terzo esempio di crimini "eventualmente" informatici[44]: in molti casi la fattispecie di reato non varia nel caso in cui venga commesso tramite tecnologie informatiche o da persone fisiche, rimane sempre lo stesso oggetto. Si parla infatti di commissione di raggiri per trarre un profitto da danni causati ad altri, e questi altri possono essere sia sistemi informatici che persone fisiche; tali persone fisiche possono essere truffate anche attraverso l'utilizzo di dispositivi informatici, ma tuttavia rimangono sempre soggetti fisici che permettono quindi di inquadrare il reato all'interno delle fattispecie di reati comuni. I casi emblematici sono quelli delle truffe attraverso lo strumento del commercio elettronico e le *advance-fee fraud*, frodi queste che implicano l'invio di denaro in anticipo con la promessa della consegna di un bene o di un guadagno attraverso fondi di investimento inesistenti[45].

Si configurano, invece, come reati puramente informatici, o più specificamente come frodi informatiche, i casi in cui viene trasferito del denaro da un conto corrente bancario online al proprio, perché in questo caso la manipolazione non interessa direttamente una persona fisica ma piuttosto un sistema informatico, quello che lavora da intermediario fra le persone fisiche e la banca. Questi reati sono disciplinati nel Codice Penale all'art. 640-*ter*, che saranno analizzate in maniera più dettagliata nel capitolo secondo.

---

[43] FLOR R., *Identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, pp. 904-908.

[44] Definizione data da AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*, Matelica, Halley Editrice, 2006 p. 50.

[45] Per un approfondimento sulle *advance-fee fraud*, BARBAGLI M. GATTI U., *La criminalità in Italia*, Bologna, Il Mulino, 2002, pp. 48 ss.

Simile alla frode bancaria, troviamo i casi di frode di identità, nel caso in cui l'hacker si impossessi dei dati della vittima per accedere ad aree riservate ed effettuare azioni illecite come la sottrazione del denaro della vittima stessa. L'*identity fraud* si configura come reato informatico nel momento in cui non viene coinvolta una persona fisica ma soltanto un dispositivo o una tecnologia, come ad esempio un archivio di dati.

Il caso del *pharming* rappresenta una via di mezzo fra reato tradizionale e informatico: questo reato può considerarsi l'evoluzione del reato di *phishing* precedentemente descritto e consiste in una tecnica di cracking utilizzata per ottenere l'accesso ad informazioni personali e riservate[46]. Nel cado del pharming, non sarà necessario convincere la vittima del reato a visitare un sito fasullo, cosa che avviene nel caso del reato di phishing, poiché sarà l'hacker stesso a modificare l'indirizzo web della pagina visitata dall'utente ignaro per fare in modo che esso venga reindirizzato su un altro sito. La vittima, credendo di trovarsi sul sito che stava cercando (come ad esempio quello della propria banca), inserisce le proprie credenziali; In questo modo, l'hacker otterrà i dati necessari ad accedere ai profili della vittima e a compiere qualsiasi tipo di operazione finanziaria a nome dell'ignaro individuo che si vedrà privato del denaro. A differenza del *phishing*, questa tecnica più tecnologicamente complessa prevede una sostanziale prevalenza del mezzo tecnologico e quindi può configurarsi come reato informatico, disciplinato all'art. 640-*ter* c.p.; il *phishing* invece viene più spesso considerato un reato di frode tradizionale (disciplinato all'art. 640 c.p.), poiché in questo caso la vittima viene portata a rilasciare le proprie informazioni di base grazie ad una truffa che lo induce in errore, e l'utilizzo del dispositivo elettronico è solo eventuale[47].

---

[46] Sul *pharming*, cfr. CAJANI F., CONSTABLE G., MAZZARACO G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008, pp. 37-38.

[47] *Ibid*; la tematica del *phishing* sarà trattata nel Capitolo II.

Infine, un altro caso emblematico di crimine impropriamente informatico è costituito dalla contraffazione delle carte di pagamento, illecito conosciuto in gergo tecnico come *skimming*, termine anglosassone traducibile letteralmente come "strisciata". Come è noto, la contraffazione di carte di pagamento è uno dei crimini più comuni e tradizionali ed esiste a prescindere dall'utilizzo delle tecnologie informatiche moderne, che non hanno fatto altro che velocizzare il processo, permettendo meccanismi più veloci di clonazione. Lo strumento necessario è il cd. *skimmer*, che una volta inserito all'interno dei lettori delle carte di credito permette di leggere e registrare i numeri di carte di pagamento e che posizionato in macchine POS, sportelli bancomat e lettori di tutti i tipi, consente la memorizzazione di un numero illimitato di carte di credito, che verranno poi riprodotte grazie a software appositi[48]. Con l'avvento delle nuove tecnologie, fortunatamente, il fenomeno dello *skimming* si sta notevolmente riducendo, soprattutto grazie all'utilizzo delle nuove carte di pagamento che funzionano grazie ad un *microchip* e non attraverso le bande magnetiche, carte di nuova generazione che rendono la tecnica dello *skimming* troppo onerosa e tecnologicamente di difficile esecuzione.

7. Aspetti tecnici e questioni irrisolte

I reati informatici per definizione agiscono su dati e programmi elettronici, intangibili e considerabili come componenti logiche di un dispositivo elettronico. Per questa ragione, vengono a mancare le categorizzazioni tradizionali dei vari elementi che tendenzialmente costituiscono ipotesi di reato, e questo pone rilevanti questioni in merito all'ordinamento giuridico che deve necessariamente tener conto della natura dei *cybercrime*. Inoltre, la continua evoluzione delle tecnologie porta ad una conseguente evoluzione dei crimini da discipli-

[48] STILO L., *Indebito utilizzo di carte di credito su Internet*, in *Nuovo dir.*, 2003, p. 262.

nare, elemento che si contrappone alla natura della legislazione che rimane sempre piuttosto rigida e difficilmente viene modificata tempestivamente.

Dal punto di vista sostanziale, ci sono una serie di elementi che creano dubbi in giurisprudenza. Il primo di essi è costituito dall'identificazione dei beni giuridici lesi da comportamenti illeciti in ambito informatico. Ma la domanda è: come si fa a comprendere i casi effettivi di illecito che vada a ledere un bene informatico? Quali sono i beni giuridici lesi? Partendo dal presupposto imprescindibile dei principi di *extrema ratio*, determinatezza e tassatività, nonché di proporzione fra l'offesa subita e la severità della pena, dottrina e giurisprudenza offrono una serie di risposte differenti nella definizione di bene giuridico per quanto riguarda i *cybercrime*. Cercare di unificare tutti i *cybercrime* sotto un unico bene giuridico, come ad esempio la "libertà informatica[49]" risulta complesso a causa della difficoltà di adattare il significato di libertà informatica a tutti i diversi reati informatici che fanno parte della categoria dei *cybercrime*. Per questa ragione, il legislatore ha inserito nel codice le fattispecie penali informatiche, preferendo non aggiungere una legge complementare, poiché i reati informatici sottendono ad una serie di beni giuridici diversi che sono gli stessi dei reati tradizionali corrispondenti, soprattutto per quanto riguarda i reati informatici "impropri". In casi come quelli del falso informatico (art. 491-*bis* c.p.) o dell'intercettazione delle comunicazioni informatiche (art. 617-*quater* c.p.), infatti, le previsioni non sono altro che aggiornamenti tecnologici di preesistenti fattispecie.

Nel caso dei reati informatici in senso stretto invece sussiste la problematica dell'individuazione del bene giuridico corrispondente in quanto non esistono reati tradizionali corrispondenti alla fattispecie informatica. In merito quindi è necessario prima di tutto distinguere fra le due tipologie di reati informatici, ossia da una parte il reato di accesso abusivo, dall'altra il danneggiamento informatico in tutte le sue forme.

---

[49] FROSINI V., *La criminalità informatica*, in *Dir. Inf.*, 1997, p. 48.

Per quanto concerne l'accesso abusivo, di cui all'art. 615-*ter* c.p.[50], la teoria più diffusa è stata recepita dalla Corte di Cassazione[51]. La Corte definisce un nuovo bene giuridico, il cd. "domicilio informatico", che altro non è che il corrispondente "virtuale" del domicilio fisico, in quanto contenente i dati registrati sul dispositivo informatico che sono protetti da misure di sicurezza. Tanto il domicilio fisico quanto il domicilio informatico, quindi, sono spazi di pertinenza dei singoli individui, che devono dunque essere tutelati alla riservatezza, ex art. 14 Cost. In base a questo principio, anche la fattispecie di reato prevista dall'art. 615-*quater* c.p.[52] garantisce la difesa della riservatezza informatica[53], poiché il legislatore persegue tutti i comportamenti che conducono all'intrusione nel sistema, non necessariamente dopo che siano già avvenute violazioni di sicurezza varie ed eventuali.

Un'altra parte della dottrina[54] non condivide il concetto di domicilio informatico, ritenendo che non è possibile condannare ogni qualsiasi intrusione all'interno di un sistema elettronico nel momento in cui non si verifichi che a questa intrusione sia seguita un'effettiva conoscenza dei dati riservati contenuti all'interno del sistema violato. In questo caso, si pone l'accento sulla riservatezza dei beni contenuti all'interno del dispositivo, non tanto sul sistema in

---

[50] L'art. 615-*ter* recita: "(*Accesso abusivo a un sistema informatico o telematico*). *Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni*".

[51] Cass. Pen., sez VI, 4 Ottobre - 14 Dicembre 1999, ric. Piersanti, pubblicata su *Cass. Pen.*, 2000, p. 2990.

[52] L'art. 615-*quater* recita: "(*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*). *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 a 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 a euro 5.164.*"

[53] PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, CEDAM, 2004, p. 63.

[54] MANTOVANI M., *Diritto penale. Parte speciale. Delitti contro il patrimonio,* Padova, CEDAM, 2009, p. 136.

sé, per evitare di tipizzare una fattispecie di reati troppo "ampia": tuttavia, questo presupporrebbe una necessaria modifica dell'art. 615-*ter*, che non considera al suo interno il concetto di dei dati contenuti all'interno di un sistema informatico.

Altra prospettiva[55] è quella che rifiuta i concetti di domicilio informatico e riservatezza, ma anche di accesso abusivo che non sia considerabile come operazione di danneggiamento di dati o del sistema violato[56]. In altre parole, l'art. 615-*ter* dovrebbe disciplinare soltanto i casi in cui l'accesso abusivo comporti un disturbo alla fruizione del dispositivo da parte del legittimo proprietario e non considerare come reati tutti gli accessi abusivi che non creino ostacoli all' "indisturbato godimento" del dispositivo. Questa prospettiva restringe di molto il campo d'azione dell'art. 615-*ter* c.p., ma tuttavia l'articolo preso in considerazione non tratta di nessun elemento di turbativa che dovrebbe essere alla base dell'incriminazione del reato di accesso abusivo; inoltre nella realtà degli avvenimenti molto spesso i soggetti che cadono vittima del reato di accesso abusivo non si rendono nemmeno conto di quello che sta avvenendo, pur potendo l'hacker accedere a documenti o sistemi che potrebbero ledere il legittimo proprietario del dispositivo.

Tuttavia, il concetto stesso di domicilio informatico presenta delle incertezze che non sono da mettere da parte: la prima di esse è che l'analogia con il domicilio fisico di un individuo è quasi impossibile da presentare nella realtà, nonostante il legislatore si sia posto nella condizione di assimilarle. Questo è un aspetto che deve essere considerato anche in relazione ai contenuti del dispositivo elettronico inteso come domicilio informatico, contenuti che in tanti casi non hanno carattere "privato" ma piuttosto economico. Inoltre, facendo riferimento alla riservatezza da garantire agli individui, bisognerebbe far rife-

---

[55] BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cass. Pen.*, 1995, p. 2339 ss.

[56] MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica*, in *Critica dir.*, 1994, n. 4, pp. 18-19.

rimento al Codice della Privacy che predispone la tutela dei dati personali a prescindere dal fatto che l'intervento avvenga attraverso sistemi informatici o meno[57]. Inoltre, un altro elemento da considerare è che l'articolo tratti di accesso ai sistemi, non ai dati: questo implica che il fulcro della disposizione non sia relativo ai contenuti del dispositivo violato, bensì alla protezione del dispositivo stesso. Quindi parlare di riservatezza informatica potrebbe creare fraintendimenti[58], in quanto l'accesso abusivo non interessa la sfera della riservatezza ma piuttosto quella della sicurezza informatica come bene giuridico. Parlare di sicurezza informatica, tuttavia, implica l'esistenza di un tipo di difesa diversa da parte del legislatore, una difesa ai dispositivi che si va ad aggiungere a quella che si presuppone essere già presente. Infatti, è l'utente il primo che deve predisporre delle misure di protezione per evitare la violazione dei propri dispositivi; nel momento in cui queste misure, che possono anche essere estremamente semplici, non si rivelano utili, allora si verifica l'intervento del diritto penale. Nel caso in cui, invece, l'utente non avesse provveduto precedentemente a predisporre delle misure di sicurezza per evitare gli ingressi non autorizzati, non è possibile interpellare l'ordinamento.

Nell'ambito del campo d'azione dell'art. 615-*quater*, invece, il bene giuridico risulta più chiaro e condiviso, ritrovandolo nel concetto di integrità informatica[59]: con questo termine, si intende la protezione di dati e sistemi dalla modifica o cancellazione abusiva. Il concetto di integrità ha ovviamente un significato ampio, intendendosi come l'insieme delle funzionalità del dispositivo ossia la sua capacità di svolgere operazioni[60]. Questo significa che in caso non

---

[57] D. lgs. 196/2003, Titolo III, Capo II, artt. 167 ss.

[58] Cfr. MANTOVANI F., *Diritto Penale. Parte speciale. Delitti contro la persona*, Padova, CEDAM, 2008, p. 533, nota n. 3.

[59] PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale del futuro,* Atti del Convegno "Il Diritto penale del futuro" (Napoli-Fisciano 17-19 sett. 2003), Napoli, Centro Stampa Fondazione Universitaria, 2006, p. 69.

[60] BERGHELLA F. - BAIOTTA R., *Diritto penale dell'informatica e beni giuridici,* in *Riv. Cass. Pen.*, 1995, p. 2341 ss.

venga danneggiato il sistema operativo ma anche solo un archivio utile perché contenente dati necessari all'utente, si tratta comunque di lesione dell'integrità informatica; le azioni che invece non alterano in maniera sostanziale il funzionamento del dispositivo (la modifica dell'aspetto grafico dello schermo, ad esempio), non vanno considerate come potenziali tipologie di reato. Il caso di aggiunta di dati falsi o estranei in un dispositivo non è da considerarsi reato, a meno che l'inserimento non abbia rilevanza dal punto di vista probatorio, poiché in questo caso va a definirsi il reato di falso informatico (art. 491-*bis* c.p.). L'elemento essenziale, in ogni caso, affinché si verifichino le condizioni tali da disciplinare il reato secondo l'art. 615-*quater*, è che il sistema alterato sia completamente o parzialmente inutilizzabile. Ovviamente il concetto di integrità e di disciplina del reato varia a seconda della tipologia di dati che vengono violati: nel caso di dati privati, in cui è una persona fisica a subire il danneggiamento, si agisce secondo una prospettiva patrimonialistica, ossia si procede tramite una querela successiva all'avvenimento illecito; nel caso di documenti di pubblico interesse, invece, si agisce anche solo dopo un attentato, perché a rischio vi è l'incolumità pubblica oltre che l'integrità informatica.

Il caso dell'art. 615-*quinquies*[61] è interessante, perché nonostante anche in questo caso si riconosca nell'integrità informatica il bene giuridico da tutelare, ci sono state una serie di modifiche all'interpretazione dell'articolo anche a seguito della legge n. 48/2008 di ratifica della Convenzione di Budapest sul *Cybercrime*, legge che ha riscritto la tipicità del reato. Infatti, originariamente

[61] L'art. 615-*quinquies* recita: "(*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*). *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, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329"*.

il testo dell'articolo[62] tendeva a punire tutti i programmi che in qualche modo portassero ad un possibile danneggiamento informatico. Era quindi stato adottato un criterio oggettivo, relativo alle caratteristiche del programma e non alle intenzioni di chi compiva l'azione, che potevano non essere necessariamente potenziali reati. L'articolo puniva indistintamente qualsiasi tipo di diffusione del *malware*, indipendentemente che questi venisse poi messo in funzione o utilizzato, o che fosse distribuito per finalità non illecite e senza l'obiettivo di danneggiare il sistema[63]. Il testo modificato dopo la Convenzione di Budapest, poi, elimina l'elemento oggettivo del potenziale danno causato dal programma, in favore dell'elemento soggettivo, ossia il dolo specifico della volontà di danneggiare un sistema. Si inserisce quindi l'elemento dell'intenzionalità di compiere un illecito ledendo l'integrità informatica, al di là della reale offensività della condotta (considerabile, appunto, l'elemento oggettivo). Ciò comporta una ulteriore anticipazione della tutela, un reato di pericolo presunto a tutti gli effetti, che difficilmente è possibile disciplinare attraverso criteri di proporzione[64]. Per risolvere questo problema, sarebbe forse necessario mantenere entrambi gli elementi del reato, sia quello oggettivo che quello soggettivo, e probabilmente anche considerare fattispecie di reato quelle relative ad una effettiva diffusione del malware, perché non sempre la detenzione di un programma dannoso si può considerare pericolosa di per sé stessa.

I due beni giuridici di cui abbiamo trattato, ossia la sicurezza e l'integrità, sono comunque separati l'uno dall'altro, perché appartenenti a due livelli distinti: infatti, mentre la sicurezza attiene al contenitore, l'integrità interessa

---

[62] Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico: *Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punto con la reclusione sino a due anni e con la multa sino a lire 20 milioni*. [Testo originario]

[63] MERLI A., *Il diritto penale dell'informatica: legislazione vigente e prospettive di riforma*, in *Giust. Pen.*, 1993, p. 119 s.

[64] SALVADORI, I., *Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive de iure condendo*, in *Ciber. Dir.*, 2008, n. 9, p. 352-353.

sostanzialmente l'interno, il funzionamento del dispositivo. Per questa ragione, ci sono delle differenze nel funzionamento della disciplina dei diversi reati, *in primis* il fatto che nel caso di danneggiamento l'assenza delle misure di protezione non costituisce elemento significativo nella disciplina del reato. Quindi la sicurezza dei sistemi e l'integrità del software al loro interno sono due elementi tutelati in maniera autonoma ed anche se sono compiuti dallo stesso soggetto non si assorbono vicendevolmente.

Sorgono inoltre altre criticità che pongono ancora oggi in difficoltà il legislatore in merito alla disciplina dei reati informatici, come ad esempio la tipizzazione delle condotte illecite. In questo caso, il legislatore ha tipizzato i reati in maniera eccessivamente casistica, cercando di comprendere tutte le ipotesi di reato possibili e immaginabili nell'ambito dei crimini informatici, senza però tener conto della difficoltà di trascurare alcuna fattispecie, soprattutto a causa del processo di evoluzione tecnologica che rende possibile la creazione di nuove tipologie di condotte illecite, che non sempre la legge riesce a seguire. Questo discorso non vale nel caso delle fattispecie su *hacking* e danneggiamento informatico, discipline che sono lasciate ad una genericità eccessiva e che a volte non tengono conto di nuovi abusi che giorno dopo giorno stanno diventando sempre più presenti nel panorama dei *cybercrime*, come ad esempio gli attacchi *DoS* o il fenomeno del *phishing*.

Altri elementi che rappresentano ancora incertezze diffuse sono quelli del *locus* e *tempus commissi delicti*, elementi sempre piuttosto fumosi nel momento in cui si tratta di reati informatici. Per quanto riguarda il *locus*, mentre la dottrina[65] riteneva che il luogo da considerare fosse quello dove si consumava l'evento, in cui si trova il dispositivo violato, la giurisprudenza[66], con una serie di sentenze, ricorda che il luogo era da considerarsi quello dove si

---

[65] FLOR R., *Art. 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. Pen. Proc.*, 2008, n.1, p. 109.

[66] Cass. Pen., sez. III, 11 Febbraio 2000, n. 5937, commentata da GENOVESE F. A., *I reati a mezzo Internet e il radicamento della giurisdizione negli stati nazionali*, in ILARDA G., MARULLO G. (a cura di) *Cybercrime: conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatica*, Milano, Giuffrè, 2004, pp. 178-179.

trovava il dispositivo da cui fosse partito l'attacco. In ultima analisi, risulta determinante una sentenza della Cassazione del Marzo 2015, in cui le Sezioni Unite hanno deliberato che il *locus commissi delicti* fosse "il luogo di consumazione del delitto di accesso abusivo del delitto di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615-*ter* c.p., è quello nel quale si trova il soggetto che effettua l'introduzione abusiva o vi si mantiene abusivamente"[67]. Per quanto riguarda il *tempus* il dubbio è sempre di difficile soluzione, data la natura stessa dei reati di cui si parla: infatti molto spesso fra l'azione che rappresenta il reato e le conseguenze che ledono effettivamente il sistema può passare del tempo. Per questa ragione il legislatore ha preferito tagliare di netto il problema stabilendo, come precisato all'art. 615-*quinquies*, che il mero possesso di software in grado di danneggiare un sistema informatico costituisca reato: in questo modo, si anticipa la risposta punitiva ad una fase precedente all'azione del malware, a prescindere da quando verrà utilizzato.

Dal punto di vista psicologico, va evidenziata la particolarità del rapporto fra l'essere umano e la macchina tecnologica, due soggetti che compiono entrambi una qualche azione passibile di sanzione e che si relazionano continuamente. Nel caso di crimini informatici, risulta inappropriato parlare di dolo[68], poiché non è la persona fisica a commettere effettivamente il reato ma dà solo un input alla macchina, che poi compirà dei processi automatizzati che non possono essere controllati dall'individuo. Casi di dolo eventuale si riscontrano solo nell'eventualità di negligenze di qualche tipo, ma solo in caso di fini repressivi. Il concetto di dolo di concorso, invece, ha una specifica ancora più complicata, dal momento che si tratta di fattispecie plurisoggettive, come nei casi degli attacchi *DDoS*, che può vedere l'azione combinata di diversi soggetti che però hanno finalità diverse, a volte non necessariamente di tipo distruttivo; o ancora, il caso in cui l'attacco sia sferrato da una serie di dispositivi

[67]Cass., Sez. Un., sent. 26 marzo 2015 (dep. 24 aprile 2015) n. 17325.

[68] PICOTTI L., *Commento all'art. 5 della l.547/1993*, in *Legisl. Pen.*, 1996, p. 122.

zombie, che reagiscono al comando di un solo artefice, che però spesso non risulta dimostrabile. Un altro elemento di difficile gestione è quello del cd. *cyber-riciclaggio*, il caso in cui si ripulisce denaro di provenienza illecita attraverso trasferimenti a conti intestati a privati, i cd. *financial manager* che accettano la partecipazione ai movimenti di denaro, con la promessa di guadagnare senza dover far altro che aprire un conto online e accettare versamenti periodici di denaro altrui; una parte di questi versamenti, sarà destinata a loro a titolo di provvigione. In merito, le decisioni hanno assunto un atteggiamento piuttosto equilibrato, definendo la liceità dell'azione del *financial manager* nel caso esso dimostri di ignorare la provenienza illecita del denaro, mentre concorre con dolo nel riciclaggio nel caso sia a conoscenza dell'attività criminale di chi lo ha ingaggiato[69]. Stesso discorso vale per gli *hacker* contattati da associazioni criminali, che sostanzialmente forniscono le proprie prestazioni, acquisendo password che poi verranno utilizzate dai criminali che gli commissionano l'azione. In questo caso vale lo stesso principio dei *financial manager*, poiché l'*hacker* che dimostri di essere inconsapevole non risponde di reato associativo o di concorso nel fatto commesso dalle organizzazioni, ma solo delle fattispecie di reato che ha effettivamente commesso, disciplinate come abbiamo visto dagli artt. 615-*ter* e 615-*quater* c.p.

La caratteristica dell'immaterialità dei reati informatici ha una serie di conseguenze anche, e soprattutto, relativamente agli aspetti processuali, specialmente riguardo le indagini e le tecniche operate per portarle avanti. Infatti, partendo dal presupposto che la vittima di un illecito informatico spesso si dimostra incerta in merito al procedere legalmente sporgendo denuncia, perché consapevole del fatto che probabilmente i suoi tentativi di trovare il responsabile si riveleranno inutili e forse addirittura lesivi della propria immagine, risulta anche molto difficile venire a conoscenza dell'identità del soggetto che agisce, visti i numerosi strumenti che permettono la garanzia dell'anonimato. I

[69] Tribunale di Palermo, 21 Aprile 2009; Tribunale di Milano, 29 Ottobre 2008; commento delle due sentenze sul sito www.antiphishing.it .

metodi più tradizionali utilizzano i *proxy server*, che fungono originariamente da schermo di protezione per garantire l'anonimato per ragioni di sicurezza, dal momento soprattutto che l'anonimato in rete non è considerabile di per se stesso un illecito ed è a disposizione di tutti gli utenti. A volte è possibile che il computer venga ritrovato, ma che appartenga a luoghi come un Internet point non in regola, dove i clienti non devono essere registrati per utilizzare i dispositivi e pertanto in sostanza rimangono comunque nell'anonimato. Altri casi sono quelli che implicano l'utilizzo di tecniche di crittografia o di rimozione degli archivi elettronici, per cancellare ogni traccia della propria ricerca o azione sul dispositivo. La tecnica di crittografia più utilizzata e di difficile decifrazione è la steganografia[70], che prima codifica un'informazione e la sua chiave di decifrazione, poi nasconde l'esistenza del file criptato, al quale si può risalire solo dopo una serie di operazioni. Quindi la stenografia è un insieme dei due metodi, quello della crittografia e quello del *wiping*[71], ossia della cancellazione degli archivi elettronici. Esiste poi lo strumento dello *spoofing*[72], che permette all'hacker di falsificare le informazioni contenute nei registri elettronici in merito ai movimenti avvenuti all'interno del sistema, senza necessità di cancellarle o criptarle. Tutti questi metodi di eliminazione o copertura delle prove non sono tuttavia impossibili da individuare: soprattutto nel caso della codificazione dei codici, esistono una serie di software che possono decodificare i sistemi, mentre si riscontrano difficoltà maggiori nei casi di *wiping*, casi che sono comunque più rari perché necessitano di un'attrezzatura più costosa e pertanto utilizzata meno frequentemente. L'elemento che va sempre tenuto in considerazione è che l'attitudine ad interessarsi in maniera maggiore o minore ai casi di crimini informatici che avvengono sfruttando

---

[70] PAIS S., PERROTTA G., *L'indagine investigativa. Manuale teorico-pratico*, Padova, Primiceri Editore, 2015, p. 275.

[71] https://en.wikipedia.org/wiki/Wiping

[72] https://en.wikipedia.org/wiki/Spoofing_attack

l'anonimato online dipende dai singoli Stati e da quanto essi siano disposti ad investire nei software e nel tempo per perseguire indagini precise[73].

Nel momento in cui viene individuato il soggetto che ha compiuto il reato si dà il via alle indagini. Queste sono da svolgersi tenendo fortemente in considerazione l'elemento della tempestività, poiché nel caso dei crimini informatici le prove risultano estremamente volatili e alterabili, o se non altro risulta piuttosto facile eliminarle e modificarle al fine di inquinarle e renderle inutilizzabili[74].

Nel contesto italiano, dove le tecniche di indagine dei reati informatici (le cd. *computer forensics*[75]) non sono molto tenute in considerazione, si tiene principalmente conto dei principi generali di legittimità, trasparenza e verificabilità[76], proprio come in tutti i casi di indagine anche in campo tradizionale, ma si riserva un'attenzione particolare all'elemento dell'integrità, perché le informazioni possono essere cambiate irrimediabilmente anche solo per errore nel corso delle indagini stesse, rendendosi inutilizzabili.

Nell'analisi del procedimento di indagine, possiamo distinguere tre passaggi-chiave: individuazione del computer da cui è stato commesso il reato,

---

[73] MOORE R., *Cybercrime: investigating high-technology computer crime*, LexisNexis Publication, 2005, p. 127 s.

[74] PECORELLA C., *Diritto penale dell'informatica*, Padova, CEDAM, 2006, p. 33.

[75] Il manuale della sez. Cybercrime del Dipartimento di Giustizia USA costituisce la guida operativa in merito alle *computer forensics*. Fonte: http://www.cybercrime.gov/ssmanual/ssmanual2009pdf

[76] La *Guide to best practice in the area of Internet crime investigation. EU Commission - Falcone Programme Training on Cybercrime investigation, Project No. JAI/2001/Falcone/127*, cita le linee guida per il trattamento delle prove digitali: a) Mai compiere azioni che possano modificare i dati nel computer se questi devono essere utilizzati in un processo penale; b) L'accesso ai dati originali è consentito solo in circostanze eccezionali e comunque il soggetto incaricato deve essere adeguatamente formato secondo gli standard UE; c) La storia delle registrazioni deve essere conservata, affinché un terzo indipendente possa esaminare tali attività investigative e giungere ai medesimi risultati (*principio della trasparenza nei metodi di indagine*); d) Applicare alle prove digitali i principi generali della Convenzione Cybercrime e tutte le regole probatorie con esse compatibili (*principio della legalità nelle indagini virtuali*); e) Incoraggiare il più possibile la collaborazione fra agenzie di nazionalità diverse, al fine dello scambio di best practices; f) L'ufficiale di polizia incaricato ha la responsabilità del rispetto di tali principi e delle regole procedurali vigenti.

acquisizione dei dati all'interno di tale computer, analisi forense delle informazioni che sono state copiate dal disco originale[77].

Nel primo passaggio è fondamentale la collaborazione degli *Internet Provider*, le società che gestiscono l'accesso alla rete e che quindi hanno a disposizione i registri che permettono di conoscere utenti che hanno avuto accesso alle reti, orari e durata dei collegamenti. Questo fenomeno, definito *data retention*, è definito all'art. 132 del d.lgs. n. 196/2003 (Codice della Privacy), in cui vengono anche definite tempistiche e modalità di consultazione del registro da parte delle varie illiceità da verificare. Nel caso si tratti di informazioni in merito alla fatturazione dell'abbonato, i registri sono conservati per sei mesi; nel caso di reati che debbano essere accertati o repressi, i termini aumentano, come è definito dal d.lgs. n. 109/2008 che modifica il Codice della Privacy distinguendo le indagini operate da un pubblico ministero rispetto a quelle operate dalle forze di polizia o dal Ministero dell'Interno. Mentre il PM può richiedere la conservazione dei dati per un anno, le forze di polizia possono farlo per 90 giorni, prorogabili a sei mesi, per svolgere indagini su reati specifici.

Ovviamente, nel momento in cui si dà inizio ad un'indagine sui dati contenuti all'interno di un registro, questi vengono congelati dal provider stesso, che non potrà compiere nessuna azione per modificarli o comunicarli a terzi, reato eventualmente disciplinato all'art. 326 c.p., *Rivelazione di segreti di ufficio*.

Passando al secondo momento dell'indagine, ossia la ricerca del materiale utilizzabile in giudizio, si può ricorrere a tre tipologie di ricerca: l'ispezione, la perquisizione o il sequestro del computer o del server. La perquisizione è il metodo di indagine più frequentemente utilizzato, con conseguente sequestro, mentre l'ispezione si rivela spesso di scarsa utilità perché consiste nell'analizzare la struttura hardware dall'esterno, senza agire sui dati ma soltanto sull'anteprima dei file e delle cartelle, senza accendere il dispositivo. La perquisizio-

[77] VACIAGO G., *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, G. Giappichelli Editore, 2012, pp. 94 ss.

ne è invece un'indagine più approfondita, trattandosi di un lavoro che agisce direttamente sui dati[78]. Queste attività sono finalizzate a ricavare le prove digitali, che sono definite come "dati informatici in grado di stabilire se un crimine è stato commesso e idonei ad individuare un fatto o una circostanza utile all'accertamento della verità processuale"[79]. Proprio a causa del carattere estremamente volatile delle informazioni e dei dati necessari alle indagini, i requisiti fondamentali che devono caratterizzare le informazioni prelevate, dai quali non si può prescindere in nessun caso, sono la genuinità e l'integrità[80], e per questa ragione le operazioni di ispezione, perquisizione e sequestro devono avvenire con la massima attenzione per evitare che i dati si perdano o vengano in qualche modo lesi nel corso dell'indagine stessa, rendendosi inutilizzabili o falsati. La soluzione migliore in tal senso è rappresentata dalla copia della memoria elettronica attraverso un programma specifico, *Encase*, che "fotografa" tutti i bit presenti sull'hard disk (effettua cioè una *bit-stream image*[81]) , creando una copia perfetta del disco sulla quale si possono effettuare le indagini in maniera approfondita senza rischiare di rovinare irrimediabilmente l'insieme di dati originale. Per non permettere che la copia venga modificata, quest'ultima si protegge inoltre con un particolare tipo di crittografia (*hashing*) che permette di scoprire ogni qualvolta si effettui una modifica dei dati sul disco o si intervenga in qualche modo su di esso, facendo in modo che la chiave

---

[78] Per le differenze fra ispezione e perquisizione di un software, cfr. ATERNO S., *Ispezioni e perquisizioni*, in CORASANITI G., CORRIAS LUCENTE G., *Cybercrime, responsabilità degli enti, prova digitale. Commento alla legge 18 Marzo 2008, n.48*, Padova, CEDAM, 2009, p. 211.

[79] CASEY E., *Digital evidence and computer crime. Forensics science, computer and the Internet*, Elsevier Academic Press, Second Edition, 2004, p. 12; la definizione originale riporta testualmente: "digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi".

[80] BRAGHO' C., *L'ispezione e la perquisizione di dati, informazioni e programmi informatici*, in LUPARIA L., *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l.18 Marzo 2008, n. 48)*, Milano, Giuffrè, 2009, p. 195.

[81] LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l.18 Marzo 2008, n. 48). Profili processuali*, in *Dir. Pen. Proc.*, 2008, n. 6, p. 219.

di accesso per accedere ai dati cambi ogni volta che i dati vengono toccati in qualche modo; il legislatore stesso ha definito il metodo *hash* come "una procedura che assicura la conformità della copia all'originale e la sua immodificabilità"[82].

Il terzo passaggio, poi, è quello dell'analisi del supporto informatico, di cui tratta anche il Codice di Procedura Penale agli artt. 359 e 360, nel quale si sottolinea la necessità di interpellare degli esperti per una consulenza tecnica e l'accertamento tecnico non ripetibile. In questa fase risulta inoltre rilevante il ruolo della difesa, che può intervenire al processo di indagine attraverso i propri consulenti tecnici effettuando ispezioni, perquisizioni ed eventuali sequestri. Questa possibilità è definita anche all'art. 233 comma 1-*bis* del c.p.p.[83], sebbene nella pratica il consulente di parte si trovi abbastanza in difficoltà poiché non può accedere a tutti i dati ma solo alla *bit stream image*, e questo non permette di sapere se la copia sia stata effettuata seguendo le corrette procedure; il consulente tecnico della difesa non potrà far altro che copiare a sua volta la fotografia di *Encase* e analizzare questa, che corrisponderà a un insieme di dati già precedentemente analizzati.

---

[82] Cfr. Art. 354 comma 2 c.p.p. "*Accertamenti urgenti su luoghi, sulle cose e sulle persone. Sequestro*".

[83] *"Il giudice, a richiesta del difensore, può autorizzare il consulente tecnico di una parte privata ad esaminare le cose sequestrate nel luogo in cui esse si trovano, ad intervenire alle ispezioni, ovvero ad esaminare l'oggetto delle ispezioni alle quali il consulente non è intervenuto. Prima dell'esercizio dell'azione penale l'autorizzazione è disposta dal pubblico ministero a richiesta del difensore. Contro il decreto che respinge la richiesta il difensore può proporre opposizione al giudice, che provvede nelle forme di cui all'articolo 127"*.

Capitolo II

La disciplina nell'ordinamento italiano

1. Origini della 547/1993

La l. n. 547/1993 è frutto della necessità per il legislatore di regolamentare e punire l'utilizzo illecito dei sistemi informatici attraverso degli interventi normativi *ad hoc* al fine di individuare dei parametri generali per la lotta ai cd. crimini informatici. Prima della l. n. 547/1993, infatti, il legislatore si era sempre mosso in maniera eccessivamente casistica, con leggi che già a partire dalla fine degli anni Settanta introducevano la tematica dei dispositivi elettronici, ma che non potevano essere considerate norme sufficientemente generali da disciplinare una serie di fattispecie di reato. È il caso, ad esempio, della l. n. 191/1978, che introduce l'art. 420 c.p. in tema di attentato ad impianti di pubblica utilità, oppure di frammentarie disposizioni all'interno di leggi, come ad esempio l'art. 12 della l. n. 197/1991 relativa alle sanzioni per il reato di uso indebito di carte di credito[84].

Tuttavia, la tutela del domicilio informatico e il sempre maggiore utilizzo delle nuove tecnologie hanno fatto sì che già negli anni Ottanta si sentisse la necessità di far riferimento ad un insieme di disposizioni penali che disciplinassero le violazioni della nuova realtà cibernetica, violazioni del tutto nuove per le loro caratteristiche di territorialità ed immaterialità. Era da chiarire, inoltre, il comportamento da adottare in merito al *locus commissi delicti*, e anche in merito alla giurisdizione competente in caso di reati transnazionali, so-

[84] NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, Jovene Editore, 2014, pp. 29 ss.

prattutto nel caso si presentassero delle discrasie fra i vari ordinamenti statuali[85].

Un' ulteriore spinta per la predisposizione della l. n. 547/1993 è derivata dalla Raccomandazione del Consiglio d'Europa del 1989 *sur la criminalitè en relation avec l'ordinateur*, che comprendeva due liste di *cybercrime*[86]*:* una, cd. lista minima, comprendeva al proprio interno tutti i reati da incriminare obbligatoriamente (frode informatica, falso in documenti informatici, danneggiamento di dati o programmi, sabotaggio informatico, accesso non autorizzato ad un sistema o ad una rete informatica, intercettazione non autorizzata con l'impiego di strumenti informatici, riproduzione non autorizzata di una topografia o di un prodotto a semiconduttori o di un programma protetto); l'altro, cd. lista facoltativa, comprendeva invece i reati punibili a discrezione dei legislatori nazionali, anche solo con strumenti di tipo amministrativo (spionaggio informatico, alterazione di dati o programmi, utilizzazione non autorizzata di un elaboratore o di un programma informatico protetto).

Il testo della Raccomandazione del 1989 diede il giusto *input* al legislatore italiano per rivedere le disposizioni penali in merito ai crimini informatici, e, per tale ragione, nello stesso anno venne formata la Commissione Callà, composta da giuristi ed esperti di informatica, che cominciò un lavoro durato quattro anni. La Commissione lavorò alla stesura di un disegno di legge, presentato in Senato il 26 Marzo 1993 dal Ministro della Giustizia Giovanni Conso, che fu poi convertito in legge il 23 Dicembre 1993, diventando la l. n. 547/1993. Tale legge si era rivelata necessaria a fronte del fatto che i reati informatici, sia che fossero configurabili come nuovi reati sia se fossero stati configurabili come reati tradizionali a mezzo informatico, costituivano una fattispecie completamente diversa rispetto a quella dei reati tradizionali: la stessa nozione di "azione" o condotta penalmente rilevante concepita come attività dell'uomo cui siano direttamente imputabili gli effetti esterni lesivi o pericolo-

[85] NERI G., *op. cit.* p. 30.

[86] Cfr. PECORELLA C., *Diritto penale dell'informatica*, Padova, CEDAM, 2006, pp. 7 ss.

si per gli interessi altrui protetti dall'ordinamento giuridico, nel *Cyberspace* si trasforma assumendo caratteristiche peculiari e complesse[87]. Per questa ragione, il legislatore ha deciso di attenersi in maniera aderente al testo della Raccomandazione del Consiglio d'Europa, comprendendo all'interno della l. n. 547/1993 sia i reati della lista minima, sia alcuni di quelli della lista facoltativa, ossia l'alterazione dei dati o dei programmi e lo spionaggio informatico. Tuttavia, è necessario precisare che i reati della lista facoltativa non sono stati inclusi all'interno della l. n. 547/1993 come reati a sé stanti, ma come elementi aggiuntivi di diversi reati informatici (ad esempio il danneggiamento) poiché non rappresentano reati sufficientemente gravi da giustificare la sanzione penale in base al criterio di *extrema ratio* e a quello di proporzionalità[88].

La nuova necessità di disciplinare i crimini informatici, inoltre, ha per un verso dato vita a norme completamente nuove, per un altro invece ha aggiornato e implementato alcune delle fattispecie di reati tradizionali, modificandone il testo. In merito, parte della dottrina considera la legge votata alla tecnica del copia-incolla, che cioè aggiunge i termini "informatica" e "telematica" a fattispecie tipiche del c.p., senza addentrarsi in una specifica analisi di beni giuridici tutelati o di comportamenti criminosi reali, o senza porsi problemi pratici di estrema rilevanza come, ad esempio, la scelta del giudice competente[89].

Il ragionamento che ha mosso il legislatore, nel momento in cui ha deciso di non emanare una nuova legge ma di aggiornare il c.p., è quello derivato dalla convinzione che le figure da introdurre non fossero altro che nuove forme di aggressione a beni giuridici già oggetto di tutela nelle diverse parti del corpo del codice. Questa decisione è stata valutata positivamente da parte del-

---

[87] PICOTTI L., *La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee*, in *Riv. trim. Dir. pen. econom.*, 2911, p. 842.

[88] Cfr. NERI G., *op. cit.* p. 30.

[89] Cfr. CORASANITI G., La tutela penale dei sistemi informatici e telematici, in www.privacy.it/cpisacoras.html .

la dottrina[90], che evidenziava le difficoltà e le incomprensioni che sarebbero potute sorgere nel momento in cui il sistema normativo fosse stato appesantito ulteriormente con una legge apposita; tuttavia altra parte della dottrina[91] avrebbe agito diversamente dedicando una legge specifica alla disciplina dei crimini informatici, ritenendo che il collegamento con il c.p. risultasse inattuale ed obsoleto per una categoria di reati nuova e diversa rispetto ai reati tradizionali.

Altri ancora hanno imputato al legislatore la mancanza di attenzione alle particolarità dei fenomeni da regolare, che per il loro carattere innovativo e le loro peculiarità dovevano essere ben differenziate rispetto ai reati tradizionali.[92]

Il legislatore è intervenuto attraverso la l. n. 547/1993 su settori estremamente eterogenei, che possono essere raggruppati in quattro grandi macrocategorie: le frodi informatiche, le falsificazioni, la lesione dell'integrità dei dati e dei sistemi e violazione della riservatezza di comunicazioni informatiche.

Le frodi informatiche sono disciplinate all'art. 640-*ter* c.p., che possono essere assimilate al reato di truffa per quanto riguarda il profilo dell'oggettività ma che tuttavia sono si caratterizzano per l'utilizzo di dispositivi informatici e quindi per l'assenza di un effettivo comportamento illecito di un essere umano, quanto piuttosto l'azione di una macchina, azione diretta a procurarsi un ingiusto profitto attraverso l'altrui danno; le cd. truffe online sono un esempio emblematico di questa fattispecie di reato.

---

[90] Cfr. BERGHELLA F. BLAIOTTA R., *Diritto penale dell'informatica e dei beni giuridici*, in *Cass. Pen.*, 1995, 2330.

[91] Cfr., fra gli altri, FONDAROLI D., *Osservazioni attorno ad alcune delle norme contenute nella recente normativa italiana sui computer crimes,* in FONDAROLI D., SOLA L. (a cura di), *La nuova normativa in materia di criminalità informatica: alcune riflessioni,* Bologna, Clueb, 1995, p. 20.

[92] Cfr., fra gli altri, NERI G., *op. ult. cit.* p. 32.

Le falsificazioni documentali sono disciplinate ai sensi dell'art. 491-*bis* c.p. nel quale si è tentata una sostanziale equiparazione fra la falsificazione di documenti informatici e quella di documenti cartacei (pubblici o privati) purché abbiano una qualche valenza probatoria. L'art. 491-*bis* c.p., inoltre, prima della modifica effettuata con l'emanazione della l. n. 48/2008, conteneva al proprio interno anche la definizione di documento informatico, ossia "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli". Per ciò che concerne invece la falsificazione del contenuto di comunicazioni informatiche, è disciplinato all'art. 617-*sexies* c.p. ed anche in questo caso la disciplina è la stessa che per la fattispecie di falsificazione del contenuto di comunicazioni telefoniche o telegrafiche, ossia che possono essere pubbliche o private purché la comunicazione falsificata venga in qualche modo utilizzata.

In merito alla lesione dell'integrità dei dati e dei sistemi informatici, in questo caso l'assimilazione al reato tradizionale di lesione dell'integrità della "cosa mobile" (disciplinato all'art. 635 c.p.) risultava piuttosto forzata in quanto il *software* non poteva far parte della categoria di "cose" definita precedentemente dalla disciplina del reato tradizionale. Per questa ragione sono stati aggiunti gli artt. 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies*, ma sono anche state modificate disposizioni preesistenti, come l'art. 392 c.p. relativo alla "violenza sulle cose"[93] e l'art. 420 c.p. in merito agli attentati ad impianti di pubblica utilità, aggiungendo anche la condotta di attentato a sistemi informatici contenenti dati, informazioni o programmi; la modifica successiva al-

[93] L'art. 392 c.p. recita: C*hiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito a querela della persona offesa con la multa fino a euro 516. Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione. Si ha altresì violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte, ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico*.

l'emanazione della l. n. 48/2008 ha però abrogato i commi aggiunti con la l. n. 547/1993[94].

Infine, per ciò che concerne la violazione della riservatezza di comunicazioni informatiche, il legislatore ha incriminato la condotta di accesso abusivo ad un sistema informatico o telematico all'art. 615-*ter* c.p., di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, ma ha anche ampliato l'ambito di operatività dell'art. 621 c.p.[95] in merito alla rivelazione del contenuto di documenti segreti, comprendendo anche quelli presenti su dispositivi informatici. Inoltre, sono state aggiunte ulteriori fattispecie di reato all'art. 617-*quater* c.p., in merito alle figure di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche, e all'art. 617-*quinquies* c.p. in merito all'installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

*2. Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter *c.p.)*

L'art 615-*ter* c.p. sull'accesso abusivo ad un sistema informatico o telematico stabilisce che "chiunque abusivamente si introduce in un sistema informatico

---

[94] L'art. 420 c.p. attualmente recita: *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*. Sono stati abrogati i commi successivi, che recitavano: *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 ad 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 ad otto anni*.

[95] L'art. 621 c.p. recita: *Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se da fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1032. Agli effetti della disposizione di cui al primo comma, è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi. Il delitto è punibile a querela della persona offesa*.

o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".

Il lessico impiegato dal legislatore è stato fortemente influenzato dall'art. 614 c.p. sulla violazione di domicilio, e a detta di parte della dottrina si percepisce una superficialità tecnica data dalla fretta di emanare la legge, fretta che ha portato ad un deficit di accuratezza per quanto riguarda il linguaggio informatico, poco utilizzato[96].

L'art. 615-*ter* c.p. comprende al proprio interno due condotte che implicano la sanzione, ossia: la prima, legata all'introduzione abusiva di un soggetto all'interno di un sistema informatico o telematico protetto da misure di sicurezza e la seconda riferita alla permanenza dell'autore dell'illecito all'interno del sistema, ugualmente protetto da misure di sicurezza, contro la volontà espressa o tacita del titolare del cd. *ius excludendi alios*. In realtà, quindi, non è solo la condotta degli hacker ad essere punita, ma anche quella di dipendenti o collaboratori che accedono legittimamente ai sistemi, in quanto titolari di codici di accesso rilasciati dal titolare, ma rimangono connessi svolgendo attività diverse da quelle per cui l'accesso è stato loro autorizzato.

In entrambe le fattispecie di reato previste dall'art.615-*ter*, un elemento che ha ulteriormente diviso dottrina e giurisprudenza si ravvisa in ciò che è comune ad entrambe le condotte, ovvero cosa si intenda per "misure di sicurezza". Parte della giurisprudenza[97] e della dottrina[98] successiva al 1993 hanno inteso in senso estremamente ampio il concetto, affermando che bastava che l'hardware si trovasse all'interno di un locale chiuso per costituire una fattispecie di reato. Questa interpretazione della nozione di misure di sicurezza appare a taluni paradossale, perché l'accesso abusivo si verrebbe a configurare

---

[96] Cfr. FROSINI V., *La criminalità informatica*, in *Dir. Informatica*, 1997, p. 487.

[97] Cass. Pen., sez. V, 6 Dicembre 2000, n.12732, in Cass. Pen., 2002, c. 1025.

[98] MANTOVANI F., *Diritto Penale. Parte speciale. Delitti contro la persona*, Padova, CEDAM, 2008, p. 518.

come reato informatico anche nel caso in cui corrispondesse, nella pratica, alla mera effrazione di una porta, all'interno della quale è possibile che i sistemi siano aperti e accessibili a tutti. In questo caso, dunque, si tratterebbe piuttosto di una violazione di domicilio (disciplinata all'art. 614 c.p.), ma non di un vero e proprio crimine informatico[99].

Si considerano dunque rilevanti tutte quelle forme di protezione fisica o logica che siano in grado di proteggere il sistema impedendone l'accesso a chi non sia autorizzato; tali misure di sicurezza, soprattutto quando si tratta di password non devono necessariamente essere violate, purché il titolare le predisponga, né devono garantire l'assoluta impenetrabilità del sistema. Non è necessario accertarsi dell'idoneità della sicurezza garantita dalla password[100] (che, in effetti, se fosse stata idonea non sarebbe stata violata), né dell'effettiva attivazione della misura di sicurezza al momento della violazione: è necessario semplicemente che il superamento delle password sia volontario e consapevole.

Circostanza aggravante, prevista al secondo comma dell'art. 615-*ter* è che l'introduzione abusiva sia effettuata all'interno di ambienti lavorativi da i cd. "operatori di sistema", comprendendo quindi all'interno della fattispecie di reato i comportamenti non autorizzati nel luogo stesso in cui si trova l'*hardware*, trattandosi in quel caso di accesso diretto. Si tratta del caso, ad esempio, in cui un impiegato si introduce all'interno di archivi elettronici ai quali non potrebbe accedere. Tuttavia, anche sulla nozione di "operatore di sistema" si sono evidenziate una serie di incertezze interpretative, che hanno diviso la dottrina. Alcuni autori ritengono che il soggetto in questione debba essere un individuo che abbia non soltanto un rapporto di fiducia con il titolare del dispositivo, abbastanza da conoscerne le password, ma che abbia anche delle

---

[99] Cfr. BORRUSO R., *Profili penali dell'informatica*, Milano, Giuffrè, 1994, p. 75.

[100] Cass. Pen., sez. V, 17 Novembre - 6 Dicembre 2000, n. 12732, Zara, su *Cass. Pen.*, 2002, pp. 1015 ss.

competenze tecniche superiori, di cui abusa per finalità illecite[101]; altri, invece, ritengono che il legislatore non abbia accennato al possedimento di capacità tecniche all'interno della disciplina e che quindi sia necessaria una visione più ampia della disposizione aggravante, che ricomprenda ogni soggetto il quale, in virtù del proprio ruolo o della propria posizione lavorativa, utilizzi il dispositivo sotto autorizzazione del legittimo proprietario[102]. Inoltre, nel caso degli accessi abusivi diretti non è quasi mai necessario avere particolari capacità tecniche per violare i dispositivi in caso si sia già operatori di sistema, in quanto spesso i dipendenti interni conoscono già i codici e le password per accedervi e non hanno bisogno di venirne a conoscenza in maniera illecita.

Un ruolo centrale nell'analisi dell'art.615-*ter* deve essere riservato alla definizione del concetto di abusività dell'accesso. Il carattere "abusivo" non viene mai definito chiaramente, ma il pensiero comune è che l'abuso consista nell'andare oltre la volontà del titolare, che essa sia manifestata espressamente o tacitamente[103]. La mancanza del consenso da parte del titolare del dispositivo è elemento necessario, che deve sussistere per tutta la durata della permanenza del soggetto agente, anche nel caso in cui l'accesso sia stato precedentemente consentito per altri scopi. Questa rappresenta la seconda fattispecie prevista dall'art. 615-*ter,* ossia il caso in cui il soggetto accede al sistema in maniera lecita, ma viola i limiti che gli erano stati imposti. Ci sono anche in questo caso una serie di specifiche e di chiarimenti da tenere presenti, per interpretare le espressioni del legislatore in modo corretto. In primo luogo, bisogna accertarsi che i file che l'agente apre in maniera illecita non siano protetti da ulteriori password, poiché in quel caso la violazione non risiederebbe nella permanenza per altri scopi diversi da quello per cui l'agente era entrato nel si-

---

[101] Cfr., fra gli altri, LUSITANO D., *In tema di accesso abusivo ai sistemi informatici o telematici*, in *Giur. It*., 1998, p. 1924.

[102] Cfr., fra gli altri, BORRUSSO R., *Profili penali dell'informatica*, Milano, Giuffrè, 1994, p. 73.

[103] Cfr. MENGONI E., *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo round alla configurabilità del reato,* Cass. Pen., 2011, 6, p. 2200.

stema, ma piuttosto nell'accesso abusivo precedentemente analizzato[104]. Inoltre, in questo caso il reato si può configurare anche nel momento in cui il soggetto agisca passivamente, ossia non disconnettendosi dal dispositivo una volta terminato il lavoro per il quale si era connesso con il permesso del titolare, ragion per cui il legislatore ha inserito all'interno della disposizione anche l'eventuale "volontà tacita" del titolare del dispositivo alla permanenza del soggetto agente all'interno del sistema[105]. L'elemento che accomuna le due fattispecie rimane comunque l'assenza del diritto da parte del soggetto agente di accedere a determinati dati all'interno del sistema, sia che acceda a quest'ultimo in maniera abusiva, sia che vi permanga dopo esservi entrato in maniera legale, ossia con l'approvazione del titolare del dispositivo[106]. Il legislatore non pone l'accento sulle motivazioni o gli scopi del soggetto agente, perché il reato si consuma nel momento dell'accesso indipendentemente da ciò che l'autore del reato farà dei dati violati[107].

Rimangono infine da chiarire tre elementi relativi alla disciplina del reato di accesso abusivo: il *tempus* e il *locus commissi delicti* e l'elemento soggettivo, ossia il dolo. Per ciò che concerne i primi due elementi, *locus* e *tempus*, è da menzionare l'intervento con cui si è espressa la Suprema Corte[108], affermando che ai fini della determinazione del luogo in cui il reato si consuma deve prendersi in considerazione il luogo in cui si entra nel sistema, che "è e non può che essere" il luogo in cui il server si trova e non "quello nel quale vengono inseriti i dati idonei ad entrare nel sistema". Per questa ragione, non sono rilevanti in merito "né il luogo in cui l'accesso al sistema è iniziato attraverso i terminali che ne costituiscono strumenti di accesso, né le eventuali condotte successive di acquisizione ed uso dei dati". Per ciò che concerne il

---

[104] Cass. Pen., sez. V, 13 Febbraio 2009, su *Mass. Pen.*, n. 243602.

[105] MUCCIARELLI F., *Commento all'art. 4 della l. 547/1993*, in *Legisl. Pen.*, 1996, p. 100.

[106] Cass. Pen., sez. II, 4 Maggio 2006, in *Dir. Pen. Proc.*, 2007, fasc. 3, p. 373.

[107] Cass. Pen., sez. V, Novembre 2000, Zara, in *Giust. Pen.*, 2001, p. 548.

[108] Sent. n. 40303 del 27 Maggio 2013, depositata in data 27 Settembre 2013.

momento in cui si perfeziona il reato, sempre nella stessa sentenza si afferma che "la procedura di accesso deve ritenersi atto prodromi alla introduzione nel sistema che avviene solo nel momento in cui si entra effettivamente nel server dopo aver completato la validazione delle credenziali dell'utente che viene fatta dal sistema centrale". I comportamenti successivi al superamento dei limiti all'ingresso o all'utilizzo del computer non riguardano la fattispecie del reato di cui all'art. 615-*ter*, ma possono tuttavia essere considerati in quanto ulteriori reati compiuti dopo l'accesso abusivo[109].

Per ciò che concerne l'elemento soggettivo, infine, nel caso dell'accesso abusivo sussiste il dolo generico, il quale consiste nella volontà e nella consapevolezza di introdursi abusivamente o di mantenersi all'interno del sistema protetto da misure di sicurezza contro la volontà espressa o tacita del titolare del dispositivo. Nel caso della permanenza, però, si configurano una serie di incertezze in merito alla consapevolezza della violazione. Per questa ragione, ci si rifà alla volontà contraria del titolare del dispositivo: nel caso tale volontà sia espressa, non si pongono dubbi; nel caso sia tacita, invece, deve essere determinata in qualche modo. In merito, parte della dottrina[110] ritiene che la presenza di password costituisca già di base la volontà contraria del titolare, senza tenere in considerazione che le barriere all'accesso sarebbero già state superate nel caso in cui si tratti di permanenza illecita all'interno del dispositivo. Altri autori[111], invece, seguono la teoria secondo cui è il soggetto che compie il reato ad essere consapevole di utilizzare il sistema per finalità diverse da quelle per cui gli era stato concesso di accedere.

Altre circostanze aggravanti sono che il reato sia commesso "da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi eserci-

---

[109] FLOR R., *Art. 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. Pen. Proc.* 2008, n.1, pp. 109-110.

[110] PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. Pen. Eco.*, 1995, p. 416.

[111] MUCCIARELLI F., *Commento all'art. 4 della l. 547/1993*, in *Legisl. Pen.*, 1996, p. 102.

ta anche abusivamente la professione di investigatore privato"[112]; che comprenda l'uso di armi o violenza sulle cose o sulle persone; che dal fatto derivi "la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti"; che i sistemi violati siano "di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interessi pubblici"[113].

*3. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici (art. 615-*quater *c.p.)*

L'art. 615-*quater* c.p. sulla detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici 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 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 fino ad un anno e con la multa sino ad euro 5164. La pena della reclusione da uno a due anni e della multa da euro 5164 a 10329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto

[112] La Cassazione ha chiarito che in questo caso il reato sia da qualificare come autonomo e distinto da quello di cui al comma 1. Cfr. Cass. Pen., sez. V, 16 Gennaio 2009, n. 1727, in *Riv. Pen.*, n. 4, 2009, p. 467.

[113] In riferimento alla circostanza aggravante dell'essere il sistema di interesse pubblico, la giurisprudenza di legittimità ha evidenziato che on è sufficiente la qualità di concessionario di pubblico servizio rivestita dal titolare del sistema, dovendosi accertare se il sistema informatico o telematico si riferisca ad attività direttamente rivolta al soddisfacimento dei bisogni generali della collettività. Cfr. Cass. Pen., sez. V, 21 Gennaio 2011, n. 1934, in dirittoitalia.it, 2012.

comma dell'art. 617-*quater*"[114]. Come è evidente, la norma è strettamente connessa a quella espressa all'art. 615-*ter*, in quanto ne costituisce una condotta anticipatoria.

La considerazione del reato di detenzione e diffusione abusiva di codici di accesso varia a seconda della definizione che si dà del concetto di bene giuridico: nel caso in cui sia inquadrato come bene giuridico il cd. domicilio informatico[115], l'art. 615-*quater* costituirebbe un reato di pericolo diretto in quanto complementare alla fattispecie definita all'art. 615-*ter*; nel caso si consideri come bene giuridico da tutelare la cd. riservatezza informatica[116], invece, il reato di cui all'art. 615-*quater* costituirebbe un reato di pericolo indiretto, ossia uno di quelli in cui il legislatore anticipa la tutela penale ad uno stadio precedente alla messa in pericolo, incrinando condotte che minano all'integrità del bene solo in via indiretta, generando pericolo di una situazione pericolosa e non effettivamente dannosa per l'interesse protetto[117]. Questa diversa prospettiva rende quindi il pericolo soltanto eventuale, ossia solo nel caso in cui i dati o i codici diffusi siano effettivamente utilizzati per scopi illeciti; per questa ragione, per la parte della dottrina che appoggia la teoria della riservatezza informatica come bene giuridico, la soglia di punibilità del reato è eccessivamente anticipata e la norma violerebbe il principio di proporzionalità che ne permetterebbe l'inserimento all'interno del c.p.[118]

---

[114] *Ex* art. 617-*quater*, punti 1) e 2) la pena è aumentata se il fatto è commesso in danno "di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità", oppure "da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore di sistema".

[115] Fra le altre, Cass. Pen., sez. VI, 4 Ottobre-14 Dicembre 1999, ric. Piersanti, in *Cass. Pen.*, 2000, p. 2990.

[116] Cfr. fra gli altri NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, Jovene Editore, 2014, p. 71.

[117] Cfr. DOLCINI E., MARINUCCI G., *Art. 615-quater*, in *Codice Penale commentato*, Milano, Ipsoa, 2006, p. 4333.

[118] Cfr., fra gli altri, NERI G., cit. pp. 72-73.

Per ciò che concerne le condotte incriminate, si tratta di due diverse fattispecie. La prima è quella relativa alla circolazione e produzione di codici d'accesso, che comprende al proprio interno le ipotesi di diffusione, comunicazione e consegna, tre condotte caratterizzate da una valenza esterna, che si verifica nel momento in cui l'informazione relativa ai codici di accesso comincia a circolare; sono inserite inoltre anche le condotte di riproduzione e acquisizione, casi in cui i dati di accesso non sono trasmessi ma semplicemente acquisiti in maniera illecita, e quindi presumibilmente antecedenti al successivo reato di accesso abusivo. Si inserisce all'interno di questo gruppo di condotte, inoltre, anche il "procurarsi" i codici di accesso, ed in merito la dottrina ha interpretato la disposizione in maniera più o meno ampia. Quest'ultima[119] sostiene che la semplice detenzione dei codici non costituisca di per se stessa reato, e pertanto non sia da configurarsi come fattispecie; solo una parte minoritaria[120] ritiene, invece, che la detenzione sia da considerarsi illecito già anticipatamente, in quanto prodromici alla condotta di accesso abusivo successivo.

Ulteriore ipotesi di reato prevede fornire indicazioni o istruzioni idonee alla produzione e alla circolazione di codici di accesso; questa ipotesi risulta ancor più anticipatoria rispetto al reato vero e proprio di accesso abusivo. Il verbo "fornisce" è volutamente scelto dal legislatore con accezione ampia, al fine di ricomprendere all'interno della definizione tutte le precedenti modalità espresse al primo comma[121]. Proprio a causa di questa ampia accezione, tuttavia, risulta necessario per una definizione più chiara della fattispecie la presenza del dolo specifico di profitto o di altrui danno, che rende più specifica la norma a fronte della vaghezza dei concetti di "fornire" e di "abusivamente"[122];

---

[119] PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. Pen. Eco.*, 1995, p. 418.

[120] MANTOVANI F., *Diritto penale. Parte speciale. Delitti contro la persona*, Padova, CEDAM, 2008, p. 254.

[121] NERI G., *op. cit.*, p. 76.

[122] PICA G., *op. cit.*, p. 417.

questa specifica determina inoltre la necessaria esistenza di finalità illecite perché si configuri il reato.

L'aspetto del *tempus commissi delicti* varia: se si tratta di una condotta divulgativa dei codici di accesso, il reato si configura nel momento in cui avviene il primo trasferimento; nel caso in cui si tratti di riproduzione, si configura nel momento in cui la copia è completa; nel caso in cui il soggetto si "procuri" il codice, il reato si perfeziona nel momento in cui entra in possesso della copia; nel caso di trasferimento di informazioni relative ai codici, infine, il reato si realizza al passaggio delle informazioni[123].

Per ciò che concerne le circostanze aggravanti, infine, la norma rimanda ai numeri 1) e 2) dell'art. 615-*quater* c.p., che comprendono al proprio interno la natura pubblicistica del sistema violato e che il soggetto che compie il reato sia un pubblico ufficiale o "un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore di sistema". Parte della dottrina[124] evidenzia l'accostamento mancato alle fattispecie di aggravanti specificate all'art. 615-*ter*, e la conseguente mancanza di fattispecie aggravante di "chi esercita anche abusivamente la professione di investigatore privato".

*4. Diffusione di programmi diretta a danneggiare o interrompere un sistema informatico (art. 615-*quinquies *c.p.)*

L'art. 615-*quinquies* c.p. nel dettato originario disponeva che "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri creato, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzio-

[123] MUCCIARELLI F., *Commento all'art. 4 della l. 547/1993*, in *Legisl. Pen.*, 1996, p. 105.

[124] NERI G., *op. cit.* p. 77.

namento, è punto con la reclusione sino a due anni e con la multa sino a lire 20 milioni". La norma è stata poi modificata a seguito dell'emanazione della l. n. 48/2008 di ratifica alla Convenzione di Budapest in materia di *Cybercrime* del 2001 e il testo modificato recita invece: "chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi 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, è punito con la reclusione fino a due anni e con la multa fino a euro 10329". Tuttavia, questa modifica successiva alla novella del 2008, per la maggioranza della dottrina[125] costituisce una mancanza da parte del legislatore. Quest'ultimo sembra essersi concentrato su aspetti che avevano poco bisogno di modifiche, dimenticandone altri, trattati all'interno della Convenzione, che continuano a rappresentare dubbi interpretativi di vario genere.

Il dolo è certamente specifico ed è rappresentato dalle condotte che precedono il danneggiamento di software o hardware, dal momento che all'interno della disposizione sono compresi gli attacchi ai programmi ma anche alle apparecchiature e dispositivi. Tuttavia l'eliminazione del requisito di pericolosità dei programmi ha avuto come conseguenza la tipicità dei reati solo in base ad un parametro soggettivo, ossia lo scopo perseguito dall'agente nel momento della diffusione del programma. Questo parametro risulta difficile da dimostrare, e risulta contrastante rispetto ai principi di determinatezza, tassatività e offensività, poiché la fattispecie sussiste in forza di un elemento psicologico e non di una circostanza esterna e verificabile concretamente[126]. In merito al bene giuridico tutelato, invece, si presentano interpretazioni diverse: secondo

---

[125] Fra gli altri, cfr. PICOTTI L., *La ratifica della Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, Padova, CEDAM, 2001, p. 719.

[126] Cfr. fra gli altri PICOTTI L., *La ratifica della Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, cit. p. 710.

parte della dottrina[127] la norma non dovrebbe inserirsi nell'ambito dei delitti contro l'inviolabilità del domicilio, al Titolo XII del c.p., ma piuttosto nell'ambito dei delitti contro il patrimonio; altri[128] sostengono invece che questo collocamento da parte del legislatore sia dovuto alla natura dei virus, che mirano ad attaccare il domicilio informatico più che singolarmente dati e informazioni.

Le condotte disciplinate dalla disposizione sono molto varie: si punisce infatti chiunque "si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione dispositivi informatici". La l. n. 48/2008 ha aggiunto una serie di condotte, estendendo di molto la fattispecie di reato poiché anche solo la circolazione del *malware* viene considerata punibile.

In merito al rapporto fra l'art. 615-*quinquies* e gli altri reati informatici, in una sentenza di merito[129] si riscontra il concorso con l'art. 615-*ter* di accesso abusivo ai sistemi informatici o telematici: il virus diffuso aveva permesso l'accesso al sistema violando le barriere all'ingresso. Per quanto riguarda invece il rapporto con l'art. 635-*quater* e *quinquies*, relativi al danneggiamento informatico, i due reati sono chiaramente interconnessi anche se risulta difficile comprendere in quale dei due momenti si realizza effettivamente la fattispecie punibile[130]; questo elemento causa ancora una serie di incertezze in giurisprudenza, poiché si presenta ancora come una "disciplina caotica"[131].

---

[127] Cfr. fra gli altri MANTOVANI F., *Diritto penale. Parte speciale. Delitti contro la persona*, Padova, CEDAM, 2011, pp. 541 ss.

[128] Cfr. fra gli altri FIANDACA G., MUSCO E., *Diritto penale. Parte speciale. Delitti contro la persona*, Bologna, Zanichelli, 2012, p. 257

[129] Trib. Bologna, 21 Luglio 2005, su *Giur. It.*, 2006, n. 5, p. 1224.

[130] DESTITO V., v. *Reati Informatici*, in *Dige. Disc. Pen. Eco.*, Aggiornam. V, 2010, p. 750.

[131] Cfr. fra gli altri MANTOVANI F., *Diritto penale. Parte speciale. Delitti contro la persona*, Padova, CEDAM, 2008, p. 508.

Un caso relativo a questa disposizione che merita di essere citato è il cd. caso "Vierika", sentenza della Cassazione Penale[132] che prende il nome dal *worm* che era stato immesso nel provider Tiscali e inviato tramite email alle vittime. Tale *virus* generava un reindirizzamento del browser con un conseguente effetto di mass-mailing, che consisteva nell'invio agli indirizzi presenti nella rubrica di Outlook di email infette e autoreplicanti. Nella sentenza di primo grado, il giudice rilevava la fattispecie di reato dell'art. 615-*ter*, considerando l'inserimento del *worm* punibile come accesso abusivo; la Corte d'Appello ha invece modificato la sentenza, applicando l'art. 615-*quinquies* poiché il *worm* presentava carattere "autoreplicante ma non infetto", e pertanto inoffensivo rispetto al bene protetto (il domicilio informatico), che non veniva danneggiato in alcun modo.

*5. Intercettazione abusiva di comunicazioni telematiche (artt. 617-*quater*, 617-*quinquies *e 617-* sexies *c.p.)*

Gli artt. 617-*quater*, *quinquies* e *sexies* regolano la tutela delle comunicazioni informatiche, proteggendo mittente e destinatario di comunicazioni digitali da interferenze di qualsiasi altro utente che abbia intenzione di violare la loro *privacy*[133]. Il messaggio deve essere in via di trasmissione e non conservato all'interno della casella di posta elettronica, reato configurabile invece all'art. 616 c.p., violazione di corrispondenza[134]. I messaggi devono essere inoltre di natura personale e rivolti ad uno o più destinatari determinati, con strumenti astrattamente idonei a mantenerne la riservatezza, come al esempio le email individuali, gli sms, ma anche i messaggi inviati ad una specifica *mailing list*,

[132] Cass. Pen., sez. III, 27 Marzo 2008, n. 369.

[133] NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, Jovene Editore, 2014, p. 81.

[134] PICOTTI L. RINALDI R., *Commento all'art. 6 della legge 547 del 1993*, in *Legisl. Pen.*, 1996, p. 118.

purché siano identificabili i partecipanti alla conversazione o alla lista. Non sono invece rilevanti ai fini della definizione della fattispecie di reato né il grado di confidenzialità del messaggio, né la forma utilizzata: potrebbe infatti "consistere in un testo scritto o, comunque, verbale, potendo meritare protezione anche un elaborato meramente grafico, fotografico o, ad esempio, di suoni digitalizzati, purché il suo significato sia sempre di messaggio ad un destinatario individuato o individuabile"[135].

I reati di intercettazione abusiva di comunicazioni telematiche fanno parte dei cd. reati "eventualmente" informatici, i quali cioè sono considerabili reati tradizionali che però si verificano attraverso l'utilizzo di dispositivi elettronici; per questa ragione, gli artt. 617-*quater*, *quinquies* e *sexies* sono la riproduzione degli artt. 617, 617-*bis* e 617-*ter,* relativi alle comunicazioni telegrafiche e telefoniche. Per questa ragione, parte della dottrina ha ritenuto la sussistenza dei *quater*, *quinquies* e *sexies* una ridondanza da parte del legislatore, a cui sarebbe potuta bastare la formulazione dell'art. 623-*bis* c.p. nella quale si stabilisce che "le disposizioni contenute nella presente sezione, relative alle comunicazioni o conversazioni, si applicano a qualunque altra trasmissione a distanza dei suoni, immagini o altri dati"[136].

5.1. Art. 617-quater *c.p.*

L'art. 617-*quater* dispone in merito all'intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche. Al primo comma si stabilisce che "chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti fra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro

[135] PICOTTI L., RINALDI R., *op. cit.*, p. 114.

[136] MANTOVANI F., *Diritto penale. Parte speciale. Delitti contro la persona*, Padova, CEDAM, 2008, p. 462.

anni"; viene incriminata dunque la condotta di intercettazione, interruzione e impedimento delle comunicazioni digitali. Per intercettazione si intende la presa di cognizione di un contenuto comunicativo, mediante intromissione nella relativa fase di trasmissione; occorre dunque l'intervenuta elusione dei predisposti dispositivi di sicurezza e la conseguente capostazione abusiva della comunicazione in corso[137]. Si verifica quindi intercettazione solo nel caso in cui la comunicazione intercettata pervenga al destinatario nella sua completezza; altrimenti, l'ipotesi è di interruzione o impedimento, sempre previsti appunto al primo comma. L'intercettazione deve inoltre avvenire, seguendo i dettami del legislatore, in maniera fraudolenta: deve trattarsi di una manomissione dell'impianto di comunicazione e deve essere ignota ai soggetti coinvolti, inconsapevoli dell'intromissione. La maggioranza della dottrina[138] ritiene che l'elemento della fraudolenza nel caso di impedimento o interruzione della comunicazione non sia necessario, perché in quel caso si tratta di aggressione alla riservatezza della comunicazione digitale, reato punibile anche in mancanza dell'atteggiamento fraudolento.

Il secondo comma punisce una seconda fattispecie di reato, autonoma[139]: "salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, in contenuto delle comunicazioni di cui al primo comma"; la divulgazione totale o parziale del contenuto delle comunicazioni telematiche costituisce una condotta a sé stante rispetto a quella disciplinata al primo comma. Per sussistere reato, quindi, è necessario il raggiungimento di un numero indeterminato di destinatari ed è inoltre necessario che il reato non sia integrato con

---

[137] CORASANITI G., *La tutela penale dei sistemi informatici e telematici*, in BORRUSO R., BUONOMO G., CORASANITI G., D'AIETTI G., *Profili penali dell'informatica*, Milano, Giuffrè, 1994, p. 121.

[138] Cfr. fra gli altri ANTOLISEI F., *Diritto penale. Parte speciale. Delitti contro la persona*, cit. p. 254.

[139] In questi casi, si parla di norma a più fattispecie o norma mista alternativa; cfr. NERI G., *op. cit.*, p. 84.

un altro più grave e punito severamente, come esplicitato dalla clausola di riserva "salvo che il fatto costituisca più grave reato"[140].

Al terzo comma, infine, vengono specificate le aggravanti di reato, in tutto simili a quelle del reato di accesso abusivo: "Tuttavia si procede d'ufficio e la pena è la reclusione da uno a cinque anni se il fatto è commesso: 1) 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; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato".

5.2. Art. 617-quinquies *c.p.*

L'art. 617-*quinquies* è invece relativo all'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche, e recita: "chiunque, fuori dei casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti fra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-*quater*".

In questo caso si presenta la volontà del legislatore di agire anticipando la disciplina del reato di cui al precedente art. 617-*quater*; infatti il reato dell'installazione di tali apparecchiature appare come un reato di pericolo, per il quale è necessario il solo accertamento dell'oggettiva potenzialità lesiva dell'apparecchiatura installata, senza la prova dell'effettiva intercettazione, interruzione o impedimento della comunicazione[141]; tuttavia, la verifica da compie-

[140] RINALDI P.G., *Commento all'art. 6 della l. 547/1993*, in *Legisl. Pen.*, 1996, p. 119.

[141] NERI G., op. cit. p. 85.

re è in merito all'idoneità delle apparecchiature installate ad intercettare effettivamente le comunicazioni, in quanto il legislatore ha voluto escludere dall'ipotesi di punibilità le apparecchiature inadatte a svolgere il reato di cui all'art. 617-*quater*[142].

5.3. Art. 617-sexies *c.p.*

L'art. 617-*sexies* relativo alla falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche, recita infine: "chiunque, 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, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-*quater*".

Con questa disposizione il legislatore aggiunge la punibilità anche per coloro i quali modifichino in qualche modo la comunicazione intercettata, falsificandola per ottenere un qualche tipo di profitto o danneggiare qualcun altro. La formulazione della disposizione ha mosso alcuni autori[143] a pensare

---

[142] AMATO G., *Commento agli articoli 617-quater, 617-quinquies*, in PADOVANI T. (a cura di), *Codice Penale*, Milano, Giuffré, 2007, p. 3815.

[143] Cfr. fra gli altri ROSSI VANNINI A., *La criminalità informatica: le tipologie di computer crimes di cui alla l. 547/1993 dirette alla tutela della riservatezza e del segreto*, in *Riv. trim. pen. econ.*, 1994, p. 451.

che ci possa essere un'analogia con gli artt. 485 e 490 c.p. relativi al falso[144]. Infatti sia nel caso dell'art. relativo ai crimini informatici che a quelli relativi al falso in generale, il reato si perfeziona non nel momento in cui avviene la falsificazione del documento o dell'informazione, ma nel momento in cui si utilizza il falso, poiché l'utilizzo è considerato elemento oggettivo del fatto[145].

6. *Danneggiamento informatico (artt. 635-*bis*, 635-*ter*, 635-*quater *e 635-*quinquies *c.p.)*

Le disposizioni relative al danneggiamento informatico introdotte con la l. n. 547/1993 entrano a far parte dell'ordinamento italiano in un contesto nel quale si sentiva forte la necessità di disciplinare reati che si verificavano a macchia d'olio, con l'esplosione del fenomeno dell'*hacking* e di movimenti terroristici che agivano attraverso episodi di danneggiamento sempre più sofisticati e complessi. Infatti, prima dell'emanazione della norma del 1993, non esisteva una disciplina che regolasse l'aggressione a dati digitali. Se da un lato la giurisprudenza adottava comportamenti contrastanti[146], dall'altro la maggioranza

---

144 L'art 485 c.p. dispone: "chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte ad una scrittura vera, dopo che questa fu definitivamente formata". L'art. 490 c.p. dispone: "chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico, o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli artt. 476, 477, 482 e 485, secondo le distinzioni in esse contenute. Si applica la disposizione del capoverso dell'articolo precedente ["qualora si tratti di scritture private chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno"]".

145 Cfr. fra gli altri PECORELLA C., sub *art. 617-sexies*, in *Comm. Dolcini Marinucci*, Milano, Giuffrè, II ed., 2004, p. 4376.

146 PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. pen. econ.*, 1995, cit. p. 420.

della dottrina[147] era abbastanza concorde nel non assimilare il reato alla disciplina dell'art. 635 c.p., relativa al danneggiamento di cose "tangibili": il *software* veniva infatti considerato un bene immateriale, che nel caso di danneggiamento comunque non sempre provocava l'inservibilità del dispositivo fisico, dell'*hardware*. Un orientamento minoritario[148] appoggiava invece la tesi dell'assimilazione all'art. 635 c.p. proprio in funzione della momentanea inservibilità che derivava dalla cancellazione totale dei dati interni. Questa inservibilità però risultava sempre difficile da dimostrare, e in secondo luogo rimaneva da risolvere la questione relativa al *locus* e al *tempus commissi delicti*, che comunque non potevano essere disciplinati come secondo la norma all'art. 635 c.p.

Per tutte queste ragioni con la l. n. 547/1993 il legislatore ha deciso di introdurre la disciplina del reato di danneggiamento informatico, prevista dal novello art. 635-*bis* c.p.; ha inoltre modificato l'art. 420 c.p.[149] relativo alla tutela impianti di pubblica utilità, che presentava gli stessi limiti dell'art. 635 c.p.[150]

A seguito della Convenzione di Budapest del 2001 e della Decisione Quadro 2005/2228 GAI dell'Unione Europea, la disciplina del danneggiamento informatico si è ulteriormente arricchita attraverso l'emanazione degli artt. 635-*ter*, 635-*quater* e 635-*quinquies* presenti nella l. n. 48/2008 di ratifica alla

---

147 Cfr, fra gli altri, PICOTTI L., *La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati*, in *Dir. Inf.*, 1986, p. 969; FIANDACA G., MUSCO E., *Diritto penale. Parte speciale*, Vol. II, Bologna, Zanichelli, 1996, p. 139.

148 Cfr. fra gli altri CORRIAS LUCENTE G., *Informatica e diritto penale. Elementi per una comparazione del diritto statunitense*, in *Dir. Inf.*, 1987, pp. 531-532.

149 A seguito della modifica, l'art. 420 c.p. 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 ad 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."

150 MUCCIARELLI F., *voce Computer (disciplina giuridica del) nel diritto penale*, in *Dige. Pen.*, vol. II, 1990, p. 288.

Convenzione sul *Cybercrime*, i quali introducono fattispecie nuove e operano una distinzione fra danneggiamento a dati o informazioni e danneggiamento a interi sistemi informatici[151].

Prima di procedere con l'analisi delle disposizioni occorre trattare il dibattito che ha diviso la dottrina in merito all'interpretazione delle disposizioni. Parte della dottrina ritiene infatti che le disposizioni siano da considerarsi nella loro accezione restrittiva, ossia solo relativamente ai danni della componente immateriale del computer; la disposizione relativa alla componente materiale, ossia l'*hardware*, si ricava all'art. 635 c.p.[152] Una minoranza ritiene invece che le disposizioni siano da interpretare nella loro accezione estensiva[153], comprendendo anche l'*hardware*; in questo caso, le fattispecie di danneggiamento informatico sarebbero state introdotte in funzione di aggravanti delle disposizioni di cui all'art. 635 c.p.[154]

*6.1. Art. 635-*bis *c.p.*

L'art. 635-*bis*, relativo al danneggiamento di informazioni, dati e programmi informatici, prevede che: "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 reclu-

---

[151] 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, CEDAM, 2009, p. 132.

[152] Cfr. fra gli altri ATERNO S., *Le fattispecie di danneggiamento informatico*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul Cybercrime (l. 18 Marzo 2008 n. 48)*, Milano, Giuffrè, 2009, p. 43.

[153] Cfr. fra gli altri PICA G., L*a disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in *Riv. Pen. Econ.*, 1995, p. 421.

[154] Favorevolmente a questa seconda ipotesi si è espressa anche una sentenza delle Sezioni Unite: Cass. Pen., Sez. Un., 13 Dicembre 1996, n. 1282, Carpanelli, in *Giur. It.*, 1997, II, pp. 647 ss.

sione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del 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 e si procede d'ufficio".

La norma mette in luce una serie di fattispecie con l'intento di evitare vuoti di tutela, cercando di non escludere nessun tipo di danneggiamento date le svariate caratteristiche peculiari dei sistemi informatici, immateriali e quindi non semplicemente "distruttibili". Per "distruzione" si deve dunque intendere l'eliminazione oggettiva della scheda di memoria contenente i dati; il "deterioramento" ne postula invece una diminuzione di funzionalità, con attacchi pregiudizievoli che ne limitano l'operatività e l'efficacia; la "cancellazione" comporta l'annientamento del programma dal suo interno, e quindi l'immissione di un virus, la smagnetizzazione del supporto magnetico o la manipolazione reversibile dei dati; l'"alterazione" ne determina la modificazione nella funzionalità originaria, in genere tramite il rimaneggiamento delle istruzioni base del programma; e da ultimo, la prevista condotta di "soppressione" costituisce di fatto una ridondante e superflua riproposizione, in termini sinonimici, delle già punite ipotesi di distruzione e cancellazione di informazioni, dati e programmi[155]; per quanto riguarda invece la definizione di "dati", "informazioni" e "programmi", la dottrina indica che per dati si intendano i *byte* in quanto unità minima della memoria, per informazioni gli aggregati di tali *byte* che forniscono contenuti, e per programmi le stringhe di comandi che indirizzano le istruzioni destinate al *software*[156]. Dopo il 2008 è stata inoltre eliminata la condotta di "rendere inservibili" i dati, le informazioni o i programmi, e questa decisione ha suscitato un parere negativo da parte della dottrina[157], in quanto

---

[155] NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, Jovene Editore, 2014, cit. p. 91.

[156] DESTITO V., *Reati informatici*, in *Dige. Disc. Pen. Eco.*, Aggiornam. V, 2010, p. 739.

[157] Cfr. fra gli altri PAGLIARO A., *Principi di diritto penale. Parte speciale. Delitti contro il patrimonio*, Vol III, Milano, Giuffrè, 2003, p. 286.

la definizione di questa condotta poteva comprendere al proprio interno tutti i comportamenti criminosi non specificamente definiti dalla norma.

Elemento importante dell'art. 635-*bis* è costituito del danno, poiché nella norma si dispone che sia "altrui": esistono dunque varie figure giuridiche che potrebbero essere considerate le persone offese dal reato, come ad esempio il proprietario, l'operatore di sistema e l'utilizzatore legittimo[158]. Il soggetto offeso ha il compito selezionare le condotte da presentare in giudizio, poiché la procedibilità della disciplina avviene per querela, e non d'ufficio (si procede d'ufficio solo nel caso di condotte aggravanti, ai sensi dell'art. 635-*bis*).

Il reato si configura come un reato di danno poiché il *tempus commissi delicti* si verifica al momento della cancellazione o dell'alterazione dei dati, anche perché l'azione è istantanea e non è possibile distinguere condotta ed evento; si presenta il dolo generico nell'elemento soggettivo, e non crea particolari incertezze interpretative.

6.2. Art. 635-quater *c.p.*

La l. n. 48/2008, aggiungendo le altre disposizioni, ha diviso la disciplina di reati che interessano il danneggiamento di dati, informazioni e programmi da quelli che interessano invece i sistemi informatici, ricompresi all'interno dell'art. 635-*quater*. Si intende con il termine "sistema informatico" l'insieme delle componenti materiali ossia l'*hardware*. In effetti, il termine indica in linea generale l'insieme delle componenti materiali e immateriali del dispositivo, ma queste ultime sono già disciplinate dall'art. 635-*bis,* e pertanto l'art. 635-*quater* si occupa nello specifico della componente fisica[159].

---

[158] PICOTTI L., *Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, n. 6, p. 711.

[159] MANTOVANI F., *Diritto penale. Parte speciale. Delitti contro il patrimonio*, Padova, CEDAM, 2009, cit. pp. 133 ss.

L'art. 635-*quater*, relativo al danneggiamento di sistemi informatici o telematici, stabilisce che: "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. Se il fatto è commesso con la violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata".

La disposizione elenca un numero ancora maggiore di condotte criminose da punire rispetto all'art.635-*bis*, in ottemperanza con il testo dell'art. 5 della Convenzione di Budapest, come se il legislatore avesse voluto attenersi in tutto e per tutto alle nuove discipline per tutelare ogni tipo di reato. Sempre per ragioni di aderenza alla Convenzione, nella quale si definiva punibile ogni comportamento atto a determinare un malfunzionamento degli elaboratori aggrediti, si è scelto di punire non solo chi rende inservibile il sistema, ma anche chi lo danneggia o lo distrugge, sebbene questa specificazione possa rappresentare un appesantimento eccessivo della norma. Ulteriore cambiamento sostanziale è rilevato nell'aggiunta della condotta di provocare "grave ostacolo al funzionamento del sistema", e parte della dottrina[160] ha rilevato che questa modifica supera un vuoto normativo in merito alla tutela nei confronti di tutti gli attacchi informatici atti a rendere momentaneamente inutilizzabili i sistemi colpiti, che però non erano configurabili come attacchi distruttivi veri e propri.

L'ultimo aspetto da considerare è relativo alle sanzioni più severe previste all'art. 635-*quater* rispetto all'art. 635-*bis*. Questa differenziazione presuppone una nitida demarcazione fra le condotte tipiche, mentre parte della dottrina evidenzia una sostanziale difficoltà interpretativa e pratica nel differenziare le due tipologie di condotte. In effetti, risulta spesso non facile stabili-

[160] Cfr. PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l.18 Marzo 2008 n. 48). Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, n. 6, p. 713.

re se un'aggressione ai dati si fermi ad essi oppure danneggi l'intera struttura informatica[161].

*6.3. Artt. 635-*ter *e 635-*quinquies *c.p.*

L'altra coppia di reati aggiunti dalla l. n. 48/2008 si può considerare speculare rispetto alle due disposizioni sopra analizzate: infatti gli artt. 635-*ter* e 635-*quinquies* trattano rispettivamente del danneggiamento a dati informatici e a sistemi informatici, ma questa volta si aggiunge l'elemento della pubblica utilità; l'introduzione di queste due nuove norme ha portato il legislatore ad abrogare il secondo e il terzo comma dell'art. 420 c.p. Questa scelta è frutto di una riflessione del legislatore relativa alla maggiore importanza da attribuire a informazioni, dati, programmi e sistemi informatici non semplicemente "altrui", ma utilizzati dallo Stato o comunque di pubblica utilità[162].

L'art. 635-*ter* relativo al danneggiamento di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, dispone: "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 sola soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secon-

---

[161] Cfr. fra gli altri NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, Jovene Editore, 2014, p. 95.

[162] Cfr. ATERNO S., *Le fattispecie di danneggiamento informatico*, in LUPARIA L. (a cura di), *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul Cybercrime (l.18 Marzo 2008, n. 48)*, Milano, Giuffrè, 2009, pp. 44 ss.

do comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Come evidenziato da parte della dottrina[163], si pone qualche dubbio interpretativo con riferimento al concetto di dati utilizzati dallo Stato nel senso che non è sufficientemente chiaro né stabilito con precisione cosa vuol dire "utilizzati" dallo Stato: questo termine dà luogo infatti ad una serie di ipotesi di utilizzo molto diverse. Inoltre, anche il concetto di "pertinenza" si rivela poco comprensibile, soprattutto poiché si sta disciplinando l'ambito informatico; si ritiene tuttavia che la pertinenza debba essere intesa come caratteristica di utilità pubblica di quel dato all'interno dei sistemi dell'ente. Ulteriore incertezza è relativa alla tipicità del reato, che si configura come reato d'attentato a causa della formulazione della disposizione che recita "chiunque commette un fatto diretto a…": in questo caso, parte della dottrina[164] sostiene che definire in questo modo la tutela abbia una natura eccessivamente anticipatoria, configurando il reato come reato consumato anche in ipotesi dove l'azione è molto lontana dall'aver determinato un pericolo al bene giuridico tutelato. Altri autori[165], invece, ritengono che dal momento che in cui si accerta l'idoneità potenziale degli atti a cancellare o alterare dati o informazioni, il pericolo si configura come concreto, e pertanto la fattispecie è già punibile.

Infine, l'art. 635-*quinquies* relativo al danneggiamento di sistemi informatici o telematici di pubblica utilità prevede che "se il fatto di cui all'art. 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, in-

---

163 ATERNO S., *op. cit.*

164 ATERNO S., *op. ult. cit.*

165 CORASANITI G., CORRIAS LUCENTE G. (a cura di), *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 Marzo 2008*, n. 48, Padova, CEDAM, 2009, p. 126.

servibile, la pena è della reclusione da tre a otto anni. Se ricorre la circostanza di cui al n. 1) del secondo comma dell'art. 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata".

Il reato, come quello previsto all'art. 635-*ter*, si configura come reato di attentato, e nonostante ciò le sanzioni previste sono più severe di quelle precedentemente previste all'art. 420 c.p. prima dell'abrogazione dei suoi commi; questo secondo alcuni è espressione della volontà del legislatore di garantire una protezione più forte ed un regime speciale più severo attraverso una norma strutturata come delitto di attentato[166].

*7. Frode informatica (art. 640-*ter *c.p.)*

L'art. 640-*ter* è stato aggiunto all'interno del c.p. dalla l. n. 547/1993 al fine di disciplinare le attività fraudolente utilizzando strumenti di tipo tecnologico. Infatti, precedentemente le truffe informatiche erano disciplinate dall'art. 640 c.p.[167], prevedendo così un'analogia della truffa informatica con la truffa tradizionale. Questa compatibilità risultava forzata alla maggioranza della dottrina[168], poiché veniva evidenziata una sostanziale differenza fra le due fattispecie: nel caso della truffa tradizionale, si prevede che una persona fisica venga tratta in inganno, mentre nel caso della frode informatica si prevede la manipolazione di un archivio elettronico. Per questa ragione, il legislatore introduce l'art. 640-*ter*, specificamente relativo alla frode compiuta attraverso tecno-

---

[166] ATERNO S., *op. ult. cit.*

[167] L'art. 640 c.p. recita: "chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altrui ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 ad euro 1032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 ad euro 1549 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità."

[168] Cfr. fra gli altri MUCCIARELLI F., *Commento all'art. 10 della l. 547/1993*, in *Legisl. Pen.*, 1996, p. 138.

logie informatiche, che dispone: "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1949 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

Gli eventi consumativi del reato rimangono gli stessi dell'art. 640 c.p., ossia il profitto ingiusto e l'altrui danno, esattamente come le sanzioni, poiché presumibilmente il legislatore ha voluto attribuire la medesima importanza ad entrambe le tipologie di frode. In merito al bene giuridico, una minoranza della dottrina[169] ritiene che l'art. 640-*ter* si autonomizzi, presentando come bene giuridico non soltanto il patrimonio, come nel caso del reato di truffa, ma anche un'altra serie di beni, ossia la riservatezza, l'integrità e l'affidabilità dei sistemi informatici; in questo senso si è espressa anche la Quinta Sezione della Corte di Cassazione in una sentenza del 1999[170]. Secondo questa dottrina, l'art. 640-*ter* non è per questa ragione assimilabile al 640 c.p., ma è strutturalmente autonomo, con proprie caratteristiche distinte dalla fattispecie che tutela la truffa tradizionale. Infatti, anche in merito alla forma, si evidenzia la cd. "forma libera" del reato di cui al 640-*ter*, attraverso l'utilizzo delle espres-

[169] Cfr. fra gli altri MARGIOCCO M., *Frode informatica*, in DELFINI F., FINOCCHIARO G. (a cura di), *Diritto dell'informatica*, Torino, UTET, 2014, p. 1108.

[170] Cass. Pen., sez. V, 24 Novembre 2003, Noto, su *Giur. It*., 2004, p. 2363.

sioni “in qualsiasi modo” e “con qualsiasi modalità”: l’induzione in errore viene in questo caso omessa poiché non si verifica il coinvolgimento di alcuna persona fisica, ma si tratta piuttosto di una cd. aggressione unilaterale[171].

La disposizione incrimina due condotte: la prima è relativa all’“alterazione del funzionamento di un sistema informatico o telematico”, ed indica una manipolazione delle funzionalità della struttura al fine di conseguire azioni fraudolente; in questo caso quindi il computer continua a funzionare, ma non come era stato inizialmente programmato, e questo elemento è importante poiché distingue la frode informatica dai delitti di danneggiamento informatico, casi in cui il sistema è danneggiato e reso inservibile. La seconda condotta è quella relativa all’intervento “senza diritto” e “con qualsiasi modalità” su dati e informazioni e programmi. Questa seconda condotta è dibattuta dalla dottrina: vi è chi pensa che sarebbe potuta bastare la condotta dell’alterazione del sistema informatico, poiché ogni intervento che potrebbe essere compreso nella seconda specificazione determina in qualsiasi caso un’alterazione già di per sé[172]; vi è, poi, chi ritiene che l’espressione “senza diritto” sia non solo ridondante ma addirittura ambigua, in quanto trattandosi di condotte illecite si tratta chiaramente di un abuso[173].

L’azione illecita può compiersi in ogni fase del processo di elaborazione dei dati o può anche incidere sul programma direttamente, modificandone le componenti. La maggioranza della dottrina ritiene che il reato sia configurabile come frode informatica, e quindi disciplinato dall’art. 640-*ter*, soltanto nei casi in cui non intervenga nessun rapporto interpersonale fra l’autore del reato e la vittima, in quanto il reato si consumerebbe attraverso processi informatici automatizzati. Tutti i reati che presuppongono tale rapporto interpersonale, anche per via telematica, sono invece da considerarsi come fattispecie di truffa

---

[171] FANELLI A., *Telefonate abusive e frode informatica*, in *Foro It*., III, 1999, p. 610.

[172] Cfr. MUCCIARELLI F., *Commento all’art. 10 della l. 547/1993*, in *Legisl. Pen*., 1996, p. 138.

[173] Cfr. PICA G., *Reati informatici e telematici*, in *Dige. Disc. Pen. Eco*., Aggiornam. I., 2000, p. 541.

tradizionale. Altri, invece, ritengono che l'utilizzo del sistema informatico o telematico basti a definire il reato sotto la fattispecie della frode informatica. Questa divisione della dottrina porta ad una diversa qualificazioni di fenomeni come quello di *phishing*, che verrà analizzato a breve, poiché tale reato si configura nel momento in cui vengono inviate ad una ignara vittima delle email fittizie da parte della propria banca, nelle quali si richiedono all'utente i propri dati personali in genere con il pretesto di problemi tecnici al sistema. Questa condotta utilizza sì il mezzo delle email, ma interessa il rapporto fra due persone fisiche, poiché la vittima è portata con l'inganno a rivelare le proprie informazioni riservate, che verranno successivamente utilizzate per ottenere "un ingiusto profitto con altrui danno".

8. Analisi e prospettive d'indagine nel fenomeno del phishing

La trattazione in merito alla disciplina dei *cybercrime* nell'ordinamento italiano deve essere conclusa con un breve approfondimento in merito ad uno dei fenomeni criminosi più diffusi in Italia, che tuttavia non presenta una disciplina giuridica *ad hoc* e che pertanto, come è già stato accennato precedentemente, presenta incertezze nell'interpretazione giuridica. Si tratta del fenomeno del *phishing*, che ha tutte le caratteristiche di una truffa attraverso dispositivi informatici[174].

Il fenomeno nasce da un meccanismo di *social engineering*, che tramite l'invio da parte di ignoti truffatori di messaggi di posta elettronica ingannevoli spinge le vittime designate a fornire volontariamente informazioni personali. Tentare di forzare il sistema centrale contenente le informazioni di migliaia di utenti risulta estremamente complesso per gli *hacker.* Viceversa, per questi ultimi risulta più semplice attaccare i singoli clienti, perché le tecnologie sono

[174] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008, pp. 14 ss.

di più semplice effrazione e anche perché l'utente medio non sempre possiede le capacità per proteggersi da eventuali attacchi.

Si distinguono sei fasi nell'attacco: il *planning*, in cui l'attaccante determina chi andrà a colpire e in che modo, per raggiungere il proprio obiettivo; il *setup*, in cui vengono configuri i meccanismi e i tools dell'attacco; l'*attack*, durante la quale cominciano i primi contatti fra l'attaccante e la vittima per indurla ad ottenere le credenziali di quest'ultima; la *collection*, il momento effettivo in cui l'attaccante ottiene i dati che cerca; la *fraud*, il momento in cui l'attaccante utilizza in qualche modo le credenziali ottenute, per rubare denaro, per effettuare un furto d'identità o per fini di riciclaggio di denaro; infine il *post attack*, fase in cui l'attaccante dopo aver terminato il proprio lavoro ne cancella le tracce[175].

Dal punto di vista della disciplina di questo fenomeno, tuttavia, come già sottolineato non esiste ancora una norma incriminatrice unica a cui ricondurre il fenomeno, ma sussistono una serie di norme evidenziate da parte della dot-

[175] CAJANI F., COSTABILE G., MAZZARACO G., *op. cit.* p. 14 ss.

trina a cui è possibile far riferimento in merito al reato[176]. A seconda delle fasi sopra descritte, infatti, si può associare al fenomeno una disciplina differente.

[176]

La prima disposizione a cui si fa riferimento[177] è all'art. 494 c.p. (sostituzione di persona), che presenta elementi oggettivi e soggettivi riscontrabili anche nel fenomeno del *phishing*; tuttavia non appare ravvisabile un riconoscimento relativo alla clausola di riserva contenuta all'art. 491-*bis* sui documenti informatici, poiché non si tratta di dati o documenti con un qualche efficacia probatoria. Altra parte della dottrina[178] associa al fenomeno l'art. 617-*sexies* (falsificazione del contenuto di comunicazione informatica), facendo riferimento al momento in cui l'autore del reato spedisce i primi messaggi ai fini di ricercare qualcuno che rilasci le proprie credenziali; tuttavia, l'ipotesi di associazione a questo tipo di disposizione viene criticata[179], poiché l'art. 617-*sexies* punisce non tanto l'azione di invio di messaggi fraudolenti, quanto più l'alterazione di messaggi precedentemente intercettati. In merito al caso in cui le credenziali vengano ottenute attraverso l'immissione nel sistema di un malware, invece, si può cercare applicazione all'art. 615-*quinquies* (diffusione di programmi diretti a danneggiare o interrompere un sistema informatico): in questo caso, si fa riferimento alla parte della disposizione in cui si parla di "alterazione del funzionamento" del sistema dopo l'utilizzo della vittima, poiché avviene un reindirizzamento su una pagina diversa da quella cercata, una pagina che abbia come scopo quello di ottenere le credenziali.

Ulteriore disposizione a cui, forse più di tutte, si può far capo nel momento in cui si disciplina il fenomeno del *phishing* è quella relativa alla truffa, in cui si rileva la suddetta divisione della dottrina per l'attribuzione del reato all'art. 640 c.p. o all'art. 640-*ter* c.p. In merito, si è espressa anche la giurisprudenza[180], optando per la soluzione che assimila il reato di *phishing* alla truffa tradizionale, dal momento che l'art. 640-*ter* richiede come condotta

---

[177] CAJANI F., COSTABILE G., MAZZARACO G., *op. ult. cit.* p. 14 ss.

[178] Cfr. fra gli altri CORASANITI G., *La tutela della comunicazione informatica e telematica* in BORRUSO R., BUONOMO G., CORASANITI G., D'AIETTI G., *Profili penali dell'informatica*, Milano, Giuffré, 1994, pp. 117 ss.

[179] Cfr. CAJANI F., COSTABILE G., MAZZARACO G., *op. ult. cit.*, p. 14 ss.

[180] Trib. Torino, 30.09.2002 in *Il diritto dell'informazione dell'informatica*, 2, 2003, p. 322.

l'alterazione di un sistema informatico, che non sussiste nel momento in cui vengono inviate email fraudolente a vittime inconsapevoli; l'eccezione potrebbe essere costituita dal fenomeno del *pharming*, nel quale effettivamente si verifica un'alterazione del sistema informatico attraverso la manipolazione dei siti internet attraverso i cd. script, delle "righe di programma" atte a modificare il contenuto di una pagina web. Nel caso in cui, invece, il reato di *phishing* sia valorizzato in quanto reato come utilizzo delle credenziali ottenute, ossia il momento successivo alla truffa per l'ottenimento delle stesse, allora è più facilmente riconducibile all'art. 640-*ter* c.p.[181]

[181] Cass. Pen., V sez., 24 Novembre 2003, n. 4576.

Capitolo III

Cooperazione internazionale nel contrasto alla criminalità informatica

1. Atti precedenti alla Convenzione di Budapest

Il concetto di stesso di prevenzione e disciplina dei reati informatici, per definizione, non può prescindere da una coordinazione sovranazionale, dal momento che il reato informatico ha carattere puramente virtuale e spesso distaccato da una qualsiasi connotazione fisica interna ad uno Stato; per questa ragione, si è rivelata necessaria una continua cooperazione internazionale per la lotta a questi reati[182].

Sebbene la Convenzione di Budapest sul *Cybercrime* del 2001 rappresenti indubbiamente la fonte più completa in merito, una vera e propria rivoluzione nel panorama europeo in materia di reati informatici poiché si tratta della prima fonte pattizia di norme che disciplinassero questo nuovo tipo di reati, i primi tentativi di regolamentazione cominciano ad affacciarsi già diverso tempo prima: si pensi che già nel 1976 si tenne a Strasburgo la prima Conferenza del Consiglio d'Europa sugli aspetti criminologici dei reati economici, nel corso della quale vennero trattati anche gli illeciti compiuti attraverso dispositivi informatici, seppure in maniera generica[183].

---

[182] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, Giuffrè Editore, 2012, p. 143.

[183] SCHJOLBERG S., *The history of Global Harmonization on Cybercrime Legislation - The road to Geneva*, 2008, p. 2. Paper consultabile al sito http://www.cybercrimelaw.net/documents/cybercrime_history.pdf .

Dieci anni dopo, nel 1986, furono emanate le Raccomandazioni OCSE che al loro interno affrontavano la disciplina di reati ed abusi avvenuti tramite le tecnologie informatiche, presentando dei concetti che non erano mai stati trattati precedentemente, nello specifico cinque: la frode elettronica (*the input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit an illegal transfer of founds or of another thing of value*), il falso informatico (*the input, alteration, erasure and/or suppression of computer data and/or computer programs made willfully with the intent to commit a forgery*), il danneggiamento di software (*the input, alteration, erasure and/or suppression of computer data and/or computer programs, or the interferenze with computer systems, made willfully with the intent to hinder the functioning of a computer and/or telecommunications system*), la violazione dei diritti di esclusivi sui programmi e processori (*the infringement of the exclusive right of the owner of a protected program with the intent to exploit commercially the program and put it on the market*), e l'accesso senza diritto "o con scopi illeciti" in un sistema informatico (t*he access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either by infringement of security measures or for other dishonest of harmful intentions*)[184]. Anche le Raccomandazioni del Consiglio d'Europa del 1989 hanno contribuito alla categorizzazione di nuove fattispecie di reati che prima non venivano tenuti in considerazione negli ordinamenti; in questo modo hanno dato l'input per l'inizio dei lavori che avrebbero poi portato alla codificazione della l. n. 547/1993, creando la giusta mentalità attorno ai nuovi illeciti ma anche attorno alle nuove figure di criminali, gli hacker[185].

Le Raccomandazioni tuttavia non trattavano in maniera precisa le questioni procedurali relative ai nuovi crimini di cui si discuteva; soltanto nel

---

[184] Cfr. OCSE, *Computer- related criminality: analysis of legal policy*, Paris 1986.

[185] Cfr. COUNCIL OF EUROPE COMMITTEE OF MINISTERS, *Recommendation No. R (89) 9 of the Committee of Ministers to Member States On Computer-Related Crime*, 13 Settembre 1989.

1995, nelle nuove Raccomandazioni del Consiglio d'Europa in materia di criminalità informatica[186], si cominciò ad analizzare la questione anche dal punto di vista procedurale stabilendo dei principi sull'andamento delle indagini nell'ambito degli strumenti informatici, fra i quali spiccano il principio di integrità e di cooperazione fra autorità giudiziarie e tecnici facenti parte delle forze di polizia.

Gli ultimi due atti precedenti alla Convenzione di Budapest sono le due Risoluzioni dell'Assemblea Generale delle Nazioni Unite, del 2000 e del 2001, che si occupano principalmente del punto di vista procedurale, facendo anch'esse perno sul principio di integrità e sulla necessità di una formazione adeguata per i tecnici che operano nel campo delle indagini informatiche.

Tutti questi atti, però, sono configurabili come fonti di *soft law*, che non ponevano in effetti alcun tipo di obbligo specifico per quanto riguardasse la disciplina dei crimini informatici, lasciando comunque libera azione ai singoli legislatori dei vari Stati e non ponendo attenzione all'elemento della cooperazione secondo una base legislativa comune sia dal punto di vista sostanziale che da quello procedurale.

2. La rivoluzione apportata dalla Convenzione di Budapest del Consiglio d'Europa

Già diversi anni prima del 2001 si era manifestata la necessità di stabilire un insieme di norme pattizie che regolassero la disciplina dei crimini informatici. Nel 1996, il Comitato Europeo sui Problemi Criminali (CDPC) - organo interno al Consiglio d'Europa composto da esperti in materie giuridiche nominati dagli Stati membri e da esperti nominati da Nazioni e Istituzioni "Osservatori" - incaricato di predisporre i presupposti per la stesura dei testi delle Conven-

[186] Cfr. COUNCIL OF EUROPE COMMITTEE OF MINISTERS, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology*, 11 Settembre 1995.

zioni ed Accordi in materia di leggi penali, nonché di adoperarsi in favore della cooperazione internazionale, aveva istituito un comitato *ad hoc* per quanto riguardava la disamina dei *cybercrime*.

Il Comitato neonato, in base alle esigenze espresse in merito alla disciplina dei reati informatici, doveva occuparsi di alcuni elementi fondamentali. Il primo di essi era rappresentato da una corretta e coerente definizione dei crimini informatici e dei comportamenti illeciti; si sentiva poi la necessità di una nuova normativa penale comune basata sulla cooperazione fra Stati, che avrebbero dovuto coordinarsi per definire le caratteristiche delle discipline dei reati informatici; la creazione di poteri coercitivi che permettessero un'indagine corretta e completa all'interno dei sistemi di rete; infine, una soluzione al problema della giurisdizione, relativamente alla determinazione del *locus commissi delicti* evitando il problema del *ne bis idem* nel caso della presenza di più di una giurisdizione, soprattutto nel caso queste non collidessero fra loro.

Il Comitato d'esperti sui Crimini in Cyber-Space (PC-CY) tenne più di dieci riunioni fra l'Aprile 1997 e il Dicembre del 2000 per redigere un atto - ossia la successiva Convenzione di Budapest - che contemplasse tutte le suddette esigenze, e un *memorandum* che sarebbe stato sottoposto all'Assemblea Parlamentare con la definizione dei punti cardine della Convenzione. Dopo l'approvazione dell'Assemblea Parlamentare, nell'Aprile 2001 e del CDPC nel Giugno dello stesso anno, si arrivò alla firma il 23 Novembre 2001 in seno al Comitato dei Ministri del Consiglio d'Europa.

2.1 Questioni sostanziali

La Convenzione di Budapest si suddivide in tre "aree di interesse": i primi articoli, infatti, vanno a specificare i reati disciplinati dalla Convenzione stessa, descrivendo una serie di comportamenti necessariamente da punire dai singoli

Stati; la seconda parte affronta le tematiche relative all'area processuale, mentre la parte finale riunisce gli articoli relativi alla cooperazione internazionale in senso stretto.

L'art. 1 della convenzione definisce la terminologia che verrà utilizzata nel corso del testo, utile perché specifica una serie di termini che ricorreranno non solo nel corso degli articoli di questo documento, ma anche all'interno delle legislazioni nazionali per i singoli Stati che hanno ratificato la Convenzione. Il concetto di "computer *system*" è il primo che viene trattato, definendolo come "ogni dispositivo o gruppo di dispositivi interconnessi, tra i quali almeno uno è programmato per eseguire processi automatici"[187]. Il termine utilizzato, sistema informatico, raggruppa al proprio interno anche la definizione di "sistema telematico", inserita all'interno dell'ordinamento italiano in maniera probabilmente ridondante. Altro termine utilizzato è quello di "computer data", definito come "qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta ai processi di un sistema informatico"[188].

A partire dall'art. 2, si susseguono le descrizioni delle varie tipologie di comportamento illecito, definendone prima di tutto le caratteristiche necessarie generali, ossia il dolo (quindi l'intenzionalità del crimine), e l'azione compiuta "senza diritto", ossia in modo abusivo o comunque senza il permesso del legittimo proprietario o di chi ne gestisce la proprietà.

Nella definizione dell'elenco dei reati di cui si interessa la Convenzione di Budapest, è importante sottolineare la distinzione fra i *cybercrime* in senso stretto e quelli in senso lato, divisi fra sezioni diverse a seconda del loro carattere intrinseco: specificamente, le prime fattispecie di reato che vengono descritte e disciplinate sono i cd. reati contro la sicurezza, l'integrità e la funzio-

[187] Definizione di computer system: "*Computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*".

[188] Definizione di computer data: "*Computer data means any representation of facts, informations or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*".

nalità dei dati e dei sistemi informatici[189], ossia i *cybercrime* in senso più tecnico[190].

L'art. 2 tratta dell'accesso abusivo, "*illegal access*"[191], ossia l'ingresso intenzionale e senza diritto ad un sistema informatico o a una parte di esso. Gli unici due elementi fondamentali sono quelli citati precedentemente, ossia il dolo e l'abusività dell'azione, mentre sono elementi solo ulteriori quelli che riguardano i fini illeciti del reperimento delle informazioni e la violazione delle misure di sicurezza che le proteggevano[192]. Nella legislazione italiana sono presenti delle evidenti differenze, dal momento che il punto focale dell'articolo corrispondente, il 615-*ter* c.p. non si preoccupa della finalità dell'accesso abusivo ma tiene fortemente in considerazione l'elemento della violazione delle barriere di sicurezza, e non sulla tematica che rappresenta il fulcro dell'art. 2 della Convenzione, ossia l'illegittimità del soggetto compiente reato di accedere al dispositivo o al sistema. Altro elemento che manca nella Convenzione è una specifica nei confronti di un illecito "reiterato", ossia nel caso in cui il soggetto che compie l'abuso rimanga all'interno di un archivio protetto per diverso tempo, elemento che nella Convenzione non configura illecito mentre nella nostra legislazione si associa al reato di violazione di domicilio[193].

Il secondo crimine facente parte dei *cybercrime* in senso stretto è quello del danneggiamento informatico, specificato nella Convenzione attraverso due diverse fattispecie disciplinate agli artt. 4 e 5. L'art. 4, nello specifico, tratta

---

189 *"Offences agsainst the confidentiality, integrity and avaiability of computer data and systems"*.

190 Cfr. SARZANA C., IPPOLITO S., *Informatica, Internet e diritto penale*, Milano, Giuffrè, 2010, p. 590.

191 Art. 2.1: "*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system*".

192 *Explanatory Report of Cybercrime Convention,* par. 44-50.

193 MUCCIARELLI F., *Commento all'art. 4 della l. 547/1993*, in *Legisl. Pen.*, 1996, p. 64.

dell'interferenza non autorizzata sui dati, *Data interference*[194], elencando tutte le possibili condotte illecite relative a questo reato, probabilmente anche in maniera troppo dettagliata e specifica; questo probabilmente perché il PC-CY, nel momento della stesura della Convenzione ha tenuto perentoriamente conto delle norme di ogni Stato, per evitare di creare dei vuoti normativi a livello sovranazionale e per questo a volte tende ad essere ridondante o ad utilizzare sinonimi o ripetizioni di concetti. Al secondo comma dell'art. 4[195], poi, viene concesso ai singoli Stati di decidere come punire il reato di danneggiamento nel caso in cui si verifichi un "grave danno"[196]. L'art. 5, invece, riguarda l'interferenza sui sistemi informatici (*System interference*[197]): si passa quindi ad un danneggiamento di un intero sistema e non di un dato singolo, apportando un "grave ostacolo" al funzionamento di tale sistema[198]. All'interno dell'articolo sono esposte in maniera lineare e chiara tutte le possibili condotte atte a causare tale illecito, differenziandole appunto dal danneggiamento di dati espresso già precedentemente all'art. 4[199]. Nel caso di un confronto con la normativa italiana, l'art. 4 è configurabile nell'art. 635-*bis* c.p., che pone una sostanziale differenza rispetto all'ordinamento comunitario, relativa alla procedibilità della fattispecie criminosa: infatti, la procedibilità si verifica tramite querela (a meno che non si verifichino le circostanze aggravanti previste al secondo

---

194 Art 4.1: *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right"*.

195 Art. 4.2: *"A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm"*.

196 *Explanatory Report of Cybercrime Convention,* par. 60-63.

197 Art. 5: *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting,transmitting, damaging, deleting, deteriorating, altering or suppressing computer data"*.

198 PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l. 18 Marzo 2008 n. 48). Profili di diritto penale sostanziale*, in *Dir. Pen. Proc*., 2008

199 *Explanatory Report of Cybercrime Convention,* par. 65-70.

comma) e quindi si lascia alla vittima la decisione di adire a vie legali, dopo aver considerato la gravità dell'illecito. Per quanto riguarda l'art. 5 invece, ritroviamo una corrispondenza con l'art. 635-*quater* c.p., che però risulta essere un mero "copia-incolla" dell'art. 5 della Convenzione aggiunto alle disposizioni già presenti nell'art. 635, creando quindi molta confusione[200].

L'art. 6 della Convenzione, *Misuse of devices*, risulta molto ampio e definisce al suo interno sia gli atti necessari ad effettuare successivamente un'operazione di accesso abusivo, sia quelli necessari invece ad effettuare un'operazione di danneggiamento informatico. La lettera *a* definisce l'insieme di condotte illecite che devono essere punite in relazione all'uso dei dispositivi[201]; la lettera *b*, poi, integra anche il reato di possesso dei dispositivi illeciti, soltanto nel caso sia possibile dimostrare l'intenzione di usarli per commettere un reato informatico[202]; dal momento che questa definizione risulta un po' aleatoria, però, ogni Stato ha la possibilità di stabilire delle soglie quantitative sotto le quali il possedimento di dispositivi illeciti non costituisce reato[203]. In Italia, il meccanismo degli artt. 615-*quater* c.p. (Detenzione e diffusione di codici di accesso) e 615-*quinquies* c.p. (In tema di apparecchiature e applicazioni dannose) è differente, considerandosi reato già il semplice possesso di

---

[200] Cfr. NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, Jovene Editore, 2014, pp. 91 ss.

[201] *Art 5: "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
a the production, sale, procurement for use, import, distribution or otherwise making available of:
i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5".

[202] *b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.*

[203] *Explanatory Report of Cybercrime Convention,* par. 71-80.

dispositivi illeciti a prescindere dall'utilizzo che si decida di farne. Dal punto di vista dell'oggetto delle condotte, l'articolo della Convenzione rimane piuttosto schematico, per lasciare margine di decisione ai singoli Stati, definendo come unica condizione il fatto che il dispositivo sia stato "progettato o adattato principalmente" con lo scopo di effettuare attività illecite nel *cyberspace*. La formulazione dell'art. 6 ha creato una serie di contrapposizioni, poiché una parte del Consiglio considerava da incriminare soltanto i programmi che erano stati creati appositamente per compiere illeciti, e l'altra che invece condannava il semplice possesso di applicazioni che potessero potenzialmente avere lo scopo di facilitare un illecito, anche se poi non sarebbero stati utilizzati per quel fine[204]. Alla fine, la disciplina che ha prevalso è stata frutto di una sorta di compromesso "forzato", poiché diventa difficile stabilire un elenco di programmi "bianchi" e programmi "neri", dal momento che tutte le applicazioni possono essere utilizzate con scopi leciti o illeciti. La valutazione empirica dei singoli casi si rivela dunque il metodo più coerente per punire volta per volta i singoli illeciti, a seconda del contesto. Proprio questo elemento rappresenta la ragione per cui nell'art. 6 viene espressa la condizione del dolo specifico di commettere un reato informatico. In Italia, invece, la disciplina di tale reato, all'art. 615 *quinquies* c.p., è molto diversa e, secondo alcuni[205], fallace: infatti nel caso italiano, il legislatore si è dimostrato troppo improntato sull'elemento oggettivo, poiché ogni applicazione o dispositivo illecito è considerato fattispecie di reato, ma anche carente di attenzione nei confronti delle garanzie all'art. 6 della Convenzione, non tenendo in considerazione le attività lecite che utilizzano o possiedono un dispositivo illecito, ma solo ai fini della sperimentazione del software criminale.

---

[204] *Explanatory Report of Cybercrime Convention*, par. 73.

[205] PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l. 18 Marzo 2008 n. 48). Profili di diritto penale sostanziale*, in *Dir. Pen. Proc.*, 2008, p. 347.

Per quanto concerne i reati eventualmente informatici, la Convenzione si esprime su diversi di essi, alcuni trattati anche nell'ordinamento italiano: è il caso di reati come quello di intercettazione abusiva nelle reti telematiche o di frode elettronica, trattati anch'essi nel loro profilo sostanziale[206].

Il reato di intercettazione di comunicazioni telematiche viene trattato all'interno dell'art. 3 della Convenzione (*Illegal Interception*[207]), e si occupa delle intercettazioni "senza diritto", avvenute tramite trasmissioni "non pubbliche" di dati digitali fra due sistemi informatici. Quando si parla di "mezzi tecnici" si fa riferimento a quelli elencati nel Rapporto ufficiale allegato alla Convenzione[208], appositamente in funzione restrittiva per evitare di penalizzare ogni forma di intercettazione in generale. Si parla inoltre di trasmissione "non pubblica", intendendo con questa definizione qualsiasi processo chiuso rispetto alle intromissioni esterne, ossia la volontà delle parti che comunicano di farlo in maniera assolutamente personale e non con la possibile aggiunta di altri soggetti[209].

L'art. 3 della Convenzione è confrontabile con l'art. 617-*quater* c.p. (Intercettazione abusiva di comunicazioni telematiche): la formulazione del nostro ordinamento pare collimare con l'ordinamento della Convenzione, e addirittura aggiunge una fattispecie di illecito nel momento in cui dopo l'intercettazione avvenga la rivelazione dei contenuti di cui si è venuti a conoscenza. L'articolo 617-*quater* definisce inoltre il reato di impedimento delle comu-

---

[206] Cfr. SARZANA C., IPPOLITO S., *Informatica, Internet e diritto penale, cit*. p. 590.

[207] Art. 3: *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system"*.

[208] *"Interception by technical means relates to listening to, monitoring or surveillance access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical communications. The may include the use of software, passwords and codes"*.

[209] *Explanatory Report of Cybercrime Convention,* par. 51-59.

nicazioni, causando un grosso danno all'operatività di un terminale[210]. All'articolo 617-*quinquies*, inoltre, viene considerata fattispecie illecita anche l'installazione di apparecchiature necessarie per l'azione di intercettazione.

L'art. 8 della Convenzione (*Computer-related fraud*[211]), che disciplina la frode informatica e che trova il suo corrispondente nell'ordinamento italiano nell'art. 640-*ter* c.p., si occupa solo di un determinato tipo di frode, ossia il danno economico altrui[212]. Nello specifico, analizza due tipi di condotta illecita, ossia la manipolazione dei dati digitali e l'interferenza nel funzionamento del sistema informatico, proprio come nell'articolo 640 *ter* c.p. Una differenza si ritrova invece nel concetto di profitto ingiusto, che nel nostro ordinamento è riconosciuto come uno dei due eventi necessari all'esistenza del reato, mentre nell'ordinamento della Convenzione è riconosciuto come oggetto del dolo, e quindi non strettamente necessario alla sussistenza del reato. Questo elemento configura da parte della Convenzione un'anticipazione della tutela penale, poiché il testo sovranazionale non tiene in considerazione la presenza o meno del profitto per definire la fattispecie di reato[213].

2.2. Questioni procedurali

Le questioni procedurali sono trattate all'interno della Convenzione agli artt. dal 14 al 22 e danno un'idea precisa e dettagliata delle metodologie di indagi-

---

[210] DESTITO V., *Reati informatici*, in *Dige. Disc. Pen. Eco.*, Aggiornam. V, 2010; CORASANITI G., CORRIAS LUCENTE G., *Cybercrime, responsabilità degli enti, prova digitale. Commento alla Legge 18 Marzo 2008, n.48*, Padova, CEDAM, 2009, p. 87.

[211] Art. 8:*"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:*
a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

[212] *Explanatory Report of Cybercrime Convention, par.* 86-90.

[213] Cfr. SARZANA C., IPPOLITO S., *Informatica, Internet e diritto penale*, cit. p. 598.

ne che devono verificarsi per reprimere efficacemente i reati informatici. I primi due articoli sono configurabili come relativi al piano dei principi, cioè che stabiliscono delle regole generali in merito all'azione da portare avanti nel momento in cui si compie un'indagine relativa ai crimini informatici[214].

L'art. 14 (*Scope of procedural provisions*), dopo aver stabilito che ogni Stato debba adottare delle misure procedurali al fine di definire specificamente i propri metodi di indagine[215], si concentra al comma 2 sulle tre tipologie di situazioni che interessano le regole procedurali, ossia i *cybercrime* descritti negli articoli precedenti, in senso stretto e in senso ampio, i reati compiuti per mezzo dei dispositivi informatici in generale, le prove raccolte in forma elettronica per un qualsiasi illecito penale[216]. Anche le prove digitali sono suddivise in tre tipologie, i dati di contenuto, i dati di traffico e i dati sugli abbonati, e il tipo di prova acquisita implica una diversa attività conseguente da parte delle forze di polizia e delle autorità giudiziarie in merito[217].

---

[214] Cfr. SARZANA C., IPPOLITO S., *Informatica, internet e diritto penale*, cit. p. 600.

[215] Art. 14.1: *"Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings"*.

[216] Art. 14.2: *"Except as a specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:*
a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
b other criminal offences committed by means of a computer system; and
c the collection of evidence in electronic form of a criminal offence".

[217] *Explanatory Report of Cybercrime Convention,* par. 140-144.

L'art. 15 (*Conditions and safeguards*[218]) definisce lo svolgimento delle attività processuali secondo le garanzie difensive all'interno dei singoli Stati, tenendo conto della piena tutela dei diritti umani e delle libertà fondamentali, nonché dei diritti civili e politici e del principio di proporzionalità. Quest'ultimo principio stabilisce che i poteri di indagine debbano essere adeguati alla natura e alle circostanze del reato, e che quindi tutte le misure compiute nei riguardi dell'imputato debbano essere strettamente limitate a quanto necessario per lo svolgimento dell'indagine[219].

L'art. 16 (*Expedited preservation of stored computer data*[220]) è il primo che si inserisce nel contesto delle regole procedurali in senso stretto, stabilen-

---

[218] Art. 15: *"1 Each Party shall ensure that the establishment, implementation and application of the*
powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties".

[219] *Explanatory Report of Cybercrime Convention, par. 146.*

[220] Art. 16: *"1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of*
specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15".

do le modalità di conservazione rapida dei dati informatici; si parla di "rapidità" in quanto gli Stati sono tenuti a mantenere in tempi brevi l'integrità dei dati elettronici necessari ai fini dell'indagine, svolgendo azioni come quella del sequestro di dati digitali o la copia crittografia dell'archivio elettronico da analizzare. Si utilizza il termine "rapido" poiché caratteristica principale dei dati informatici è la loro volatilità, che rende assolutamente necessaria un'azione celere. Per quanto riguarda l'integrità dei dati, è possibile anche effettuare una copia clonata dell'archivio per evitare di rendere l'originale inaccessibile anche ai legittimi proprietari, purché la copia garantisca affidabilità e autenticità[221]. Ulteriore elemento sottolineato dall'articolo 16 è quello della segretezza rispetto all'operazione e il divieto per il custode degli archivi di modificare o alterare le prove.

L'art. 17 è relativo alla conoscenza parziale dei dati di traffico (*Expedited preservation and partial disclosure of traffic data*[222]), definiti precedentemente all'art. 1 lettera d come tutti i dati relativi ad una comunicazione per mezzo di sistemi informatici, che formano una rete interconnessa: nello specifico, ci si riferisce all'origine, la destinazione, il percorso, la data, le dimensioni e la tipologia di comunicazione. L'art. stabilisce la necessità di una rapida conservazione dei dati di traffico, e impone ai provider la rivelazione di tali dati per collaborare ai fini dell'indagine penale. L'Italia, dopo aver ratificato la Convenzione, si è adeguata a questo obbligo in capo ai provider[223], aumentan-

---

[221] *Explanatory Report of Cybercrime Convention*, par. 159.

[222] Art. 17: *"1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:*
a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15".

[223] Codice della Privacy, art. 132 comma 4 *ter*, d.lgs. 196/2003.

do la durata della cosiddetta *data retention*, ossia il periodo in cui i dati debbano essere conservati, che può sussistere fra i tre e i sei mesi.

L'art. 18 tratta invece della produzione alle autorità di dati nella disponibilità di privati (*Production order*), prendendo in considerazione i dati sugli abbonati, descritti al terzo comma[224]: sono le informazioni gestite da un ISP riguardanti gli abbonati, sia dal punto di vista del contratto o del servizio sottoscritto, sia da quello delle generalità. L'art., dunque, si interessa di dati già presenti all'interno degli archivi elettronici, richiedendo ai provider una collaborazione minimale, semplicemente attraverso la messa a disposizione delle autorità i dati archiviati precedentemente al fine di favorire le indagini[225]. A seguito della ratifica della Convenzione di Budapest, l'ordinamento italiano ha subìto una forte innovazione relativamente alla responsabilità del provider, poiché si dispone all'art. 254-*bis* c.p.p. a proposito del "sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni". Il sequestro deve essere effettuato per acquisire i dati necessari alle indagini, ma nel caso questa azione giudiziaria presupponesse il blocco dei servizi Internet è necessario copiare l'archivio da sequestrare per analizzare la copia; il provider comunque è responsabile dell'archivio, affinché non venga alterato da terzi.

L'art. 19 (*Search and seizure of stored computer data*) si occupa dei vari istituti che regolano le indagini informatiche, e si divide fra varie analisi: al primo e secondo comma si ritrovano l'accesso e la ricerca a sistemi informati-

---

[224] Art. 18.3: *"For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*
a the type of communication service used, the technical provisions taken thereto and the period of service;
b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement".

[225] *Explanatory Report of Cybercrime Convention*, par. 181.

ci e dati digitali, nel terzo comma si tratta dei provvedimenti di sequestro, ed infine nel quarto comma si affronta l'analisi del problema delle barriere di sicurezza che bloccano il sistema da analizzare[226].

Al primo e al secondo comma[227], l'art. 19 ribadisce il potere ispettivo delle autorità nel corso di indagini informatiche, ma impone anche l'estensione dell'oggetto delle attività investigative e dei provvedimenti anche ad altri computer qualora si ritenesse necessario, lasciando sostanzialmente carta bianca alle legislazioni interne agli Stati in merito agli atti adottabili. Tuttavia, questo profilo di estensione della disciplina delle indagini deve essere tenuto in considerazione solo per quanto riguarda le indagini interne ai singoli Stati: nel caso di indagini che interessino più Paesi (nel caso di reati transnazionali), si applicano le regole della cooperazione internazionale, che verranno trattate successivamente. Al terzo comma[228], invece, in merito alle misure relative al sequestro si ribadisce l'importanza del mantenimento dell'integrità dei dati e le modalità di indagine tramite sequestro degli archivi o copia della memoria, che comunque deve essere effettuata in tutti i casi per procedere alle indagini senza rischiare di alterare i dati contenuti all'interno degli archivi; questo av-

---

[226] Fonte: *Explanatory Report of Cybercrime Convention,* par. 184-204.

[227] Art. 19.1 e 19.2: *"1 Each Party shall adopt such legislative and other measures as may be necessary to*
empower its competent authorities to search or similarly access:
a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored in its territory.
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system".

[228] Art. 19.3: *"Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:*
a seize or similarly secure a computer system or part of it or a computer-data storage medium;
b make and retain a copy of those computer data;
c maintain the integrity of the relevant stored computer data;
d render inaccessible or remove those computer data in the accessed computer system".

viene tramite la già citata tecnica della *bit-stream image*. Il quarto comma[229] dell'art. 19 della Convenzione, infine, si sofferma sul ruolo dei privati nel corso delle indagini, che sono tenuti a collaborare fornendo le informazioni relative a dati e password di cui sono a conoscenza per consentire il corretto svolgimento delle indagini e l'analisi degli archivi elettronici.

L'ordinamento italiano post-ratifica ha subìto un cambiamento significativo[230], poiché si sono esplicitate all'interno del Codice di Procedura Penale (artt. 244, 247 e 248) le possibilità di effettuare ispezioni e perquisizioni anche relativamente ai sistemi informatici, seguendo gli standard operativi delle cd. *computer forensics*. Inoltre si stabilisce la necessità di prendere misure adeguate per garantire l'autenticità del *software*, ma soprattutto si prevede la possibilità per le autorità investigative di munirsi di mezzi tecnici al fine di superare le barriere d'accesso ai sistemi informatici protetti ai fini di effettuare le dovute analisi[231].

Gli artt. 20 e 21 si inseriscono all'interno dell'ambito delle intercettazioni telematiche; nello specifico, l'art. 20 (*Real-time collection of traffic data*) si riferisce alla raccolta dei dati di traffico in tempo reale, mentre il 21 (*Interception of content data*) all'intercettazione delle comunicazioni telematiche da parte dei provider. A tali disposizioni possono essere apposte delle riserve *ex* art. 14 della Convenzione, definite dai singoli Stati per restringere il campo delle intercettazioni a categorie di reati più gravi; l'Italia non ha sotteso a que-

---

[229] Art. 19.4: *"4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2"*.

[230] Cfr. LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l. 18 Marzo 2008, n. 48). Profili processuali*, in *Dir. Pen. Proc.*, 2008, n.6, p. 719.

[231] L'art. *352.1-bis* c.p.p. stabilisce*:* "Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi".

sta norma, quindi le intercettazioni possono essere utilizzate per indagini in merito a qualsiasi fattispecie criminosa commessa in relazione a sistemi informatici.

L'ultima disposizione relativa agli aspetti procedurali della Convenzione di Budapest è contenuta all'art. 22 che tratta una tematica estremamente delicata, ossia quella della determinazione della giurisdizione. Questo stabilisce che un reato possa essere perseguito per legge da uno Stato nel momento in cui si considera il territorio nazionale oppure la cittadinanza del soggetto che ha commesso il reato, nel momento in cui questo viene commesso fuori dallo Stato di appartenenza. Tuttavia, questo causa numerosi problemi nei singoli Stati in merito a conflitti di giurisdizione, ma anche difficoltà di definizione del luogo dove viene commesso il reato che, come abbiamo più volte ripetuto, risulta di difficile "collocazione spaziale". La Convenzione non specifica nessuna soluzione a questi dubbi, mantenendosi prudente e facendo solo riferimento alla necessità di cooperazione fra gli Stati e lasciando aperta l'ipotesi di consultazioni fra di essi; nel caso in cui questa ipotesi di dialogo non si rivelasse possibile, la Convenzione non offre altre ipotesi di soluzione[232].

2.3. Cooperazione fra Stati

La tematica relativa alla transnazionalità dei reati informatici e della conseguente necessità di una cooperazione fra i diversi Stati è centrale negli artt. dal 23 al 35 della Convenzione di Budapest. In questa parte, il Consiglio ha elencato una serie di principi e di disposizioni affinché si rendesse possibile la massima coordinazione nelle azioni dei vari Paesi[233].

È necessario però evidenziare subito la scarsa esecuzione di tali disposizioni all'interno dell'ordinamento italiano, poiché il nostro Paese ha ratificato

[232] *Explanatory Report of Cybercrime Convention,* par. 232-239.

[233] Cfr. SARZANA C., IPPOLITO S., *Informatica, Internet e diritto penale*, cit. p. 615.

nella l. n. 48/2008 soltanto una piccola parte degli articoli relativi a questo argomento nella Convenzione di Budapest, perdendo un'occasione per semplificare in maniera profonda le norme in merito ad un argomento spinoso come quello della cooperazione internazionale. Le disposizioni che l'Italia ha ratificato sono infatti soltanto di portata più generale, che possono essere compatibili con quelle rintracciabili all'interno del Libro Undicesimo del c.p.p.[234], corrispondenti agli artt. 23, 24, 25, 27 e 29 della Convenzione.

Gli artt. 23, 24 e 25 sono stati pienamente riconosciuti all'interno dell'ordinamento italiano, e trattano della cooperazione durante il corso delle indagini investigative fra Paesi con giurisdizioni diverse; nello specifico, l'art. 23 (*General principles relating to international cooperation*) invita gli Stati a cooperare nel miglior modo possibile alle indagini, abbastanza genericamente; l'art. 24 (*Extradition*) tratta della tematica dell'estradizione, trattando dei casi in cui alcuni Paesi siano favorevoli all'estradizione mentre altri non lo siano, e lasciando un margine decisionale abbastanza ampio agli Stati; l'art. 25 (*General principles relating to mutual assistance*) invece tratta più in particolare della mutua assistenza nella raccolta di prove digitali necessarie alle indagini, che deve essere incentivata e favorita in ogni caso. Nel caso in cui uno Stato rifiuti la collaborazione, deve motivare la propria scelta, anche se la Convenzione pone dei casi in cui i rifiuti anche motivati debbano essere considerati inammissibili, per esempio nel caso della "doppia incriminazione", per cui entrambi gli Stati riconoscano il fatto in questione come una fattispecie di reato[235].

Gli artt. 27 (*Procedures pertaining to mutual assistance requests in the absence of applicable international agreements*) e 29 (*Expedited preservation of stored computer data*) sono le ultime disposizioni che trovano applicazione anche all'interno della legge di ratifica italiana, e trattano rispettivamente della

---

[234] COLOMBO E., *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in *Ciber. Dir.* 2009, n. 3-4

[235] *Explanatory Report of Cybercrime Convention*, par. 241-259.

mutua assistenza in mancanza di accordi internazionali applicabili e della procedura sin merito alla raccolta dei dati informatici all'estero. L'art. 27 ha validità soltanto nel momento in cui gli Stati non abbiano precedentemente predisposto un accordo, e stabilisce una serie di norme "basilari" per sopperire alla mancanza di tali accordi in caso di necessità di cooperazione fra gli Stati; fra le disposizioni centrali figurano la possibilità di mantenere segrete le operazioni di cooperazione alle indagini, ma anche la disciplina in merito alle richieste di assistenza, che devono essere sempre soddisfatte come richiesto dallo Stato richiedente, a meno che tali modalità non siano considerate incompatibili con l'ordinamento interno dello Stato che debba accettare la richiesta. In questo caso (si tratta dunque di una disciplina residuale), si possono verificare due conseguenze: o che le modalità della richiesta cambino, diventando quelle dello Stato che deve accettare la richiesta, oppure che lo Stato respinga direttamente la richiesta di assistenza, se ritiene il reato in questione un reato di natura polita oppure che questa richiesta pregiudichi in qualche modo gli interessi nazionali essenziali. Un'alternativa al rifiuto della richiesta è la sospensione temporanea, nel caso in cui la richiesta di assistenza rischi di provocare un intralcio ad un'altra indagine penale in corso. E' sempre vivamente consigliato, in ogni caso, il dialogo fra Stato richiedente e Stato richiesto, al fine di raggiungere un compromesso e un'intesa[236].

L'art. 29 affronta un tema più specifico, quello della conservazione rapida di dati informatici, che può essere considerato un aspetto della tematica più generale della mutua assistenza; le disposizioni in merito sono dunque le stesse previste all'art. 27, comprese anche le possibili ragioni di rifiuto da parte dello Stato richiesto di accettare la richiesta di cooperazione. Fra le disposizioni, risultano importanti quelle relative alla durata della conservazione dei dati, che non deve mai essere inferiore ai sessanta giorni e che comunque deve sussistere fintanto che sussiste la necessità da parte dello Stato richiedente[237].

---

[236] *Explanatory Report of Cybercrime Convention,* par. 262-274.

[237] *Explanatory Report of Cybercrime Convention,* par. 282-289.

Per quanto riguarda gli artt. 26, 28, 30, 31, 32, 33 e 34, relativi alla mutua assistenza giudiziaria, essi non sono stati introdotti nell'ordinamento italiano dopo la ratifica del 2008 e pertanto non hanno corrispondenza interna; gli artt. 26 e 28, specificamente, si occupano dello scambio di dati e informazioni fra Stati, nel primo caso dati comunicati spontaneamente poiché pubblici, nel secondo invece previa richieste e vincoli di vario genere a causa delle caratteristiche di sensibilità e confidenzialità dei dati. Gli artt. dal 30 al 34 invece sono disposizioni più specifiche relative all'ambito della mutua assistenza, come acquisizione rapida di dati di traffico (art. 30, *Expedited disclosure of preserved traffic data*), accesso ad informazioni archiviate in forma elettronica (art. 31, *Mutual assistance regarding accessing of stored computer data*), accesso transfrontalieri a sistemi informatici aperti al pubblico o con il consenso dello Stato territoriale (art. 32, *Trans-border access to stored computer data with consent or where publicly available*), raccolta in tempo reale di dati di traffico (art. 33, *Mutual assistance in the real-time collection of traffic data*) e intercettazione di dati di contenuto (art. 34, *Mutual assistance regarding the interception of content data*).

3. La l. n. 48/2008 di ratifica alla Convenzione sul Cybercrime

Il percorso che ha portato alla ratifica della Convenzione di Budapest da parte dell'Italia comincia l'11 Marzo 2007 con l'approvazione da parte del Presidente del Consiglio dei Ministri dello schema di disegno di legge recante autorizzazione alla ratifica della Convenzione del Consiglio d'Europa sulla criminalità informatica, sottoscritta a Budapest il 23 novembre 2001, e la sua esecuzione nonché le norme di adeguamento dell'ordinamento interno. Nel Giugno dello stesso anno, il governo presenta l'atto alla Camera dei Deputati, e successivamente l'atto viene assegnato alle Commissioni Riunite II (Giustizia)

e III (Affari esteri), in sede referente il 24 luglio 2007 con pareri delle commissioni I, V, VI, VII e IX e viene esaminato dalla III commissione il 25 settembre 2007; 3 ottobre 2007 e 19 febbraio 2008. In quest'ultima data il d.d.l. viene presentato in aula, secondo alcuni con eccessiva frettolosità data dalla decisione di ratificare la Convenzione durante il periodo di *prorogatio*, poco prima dello scioglimento delle Camere[238]. Questa improvvisa accelerazione spiazza i membri della Commissione che non avevano ancora terminato i lavori di approfondimento su alcune disposizioni; tuttavia, il 20 Febbraio 2008 dopo una serie di dibattiti in aula, il testo viene approvato. Dopo il passaggio al Senato, avvenuto anch'esso rapidamente, il 18 Marzo la legge n. 48 viene firmata dal Presidente della Repubblica.

L'intervento attuativo, se da un lato ha conformato l'ordinamento agli obblighi pattizi sovranazionali della Convenzione, dopo ben sette anni di attesa, dall'altro ha deluso le aspettative della dottrina, forse soprattutto a causa della sopracitata "fretta" che la commissione ha dimostrato di avere, di ratificare la Convenzione di Budapest prima della caduta del Governo Prodi[239].

La l. n. 48/2008, oltre ad aver modificato una serie di articoli del c.p. introdotti precedentemente dalla l.n. 547/1993, soprattutto in ambito sostanziale ossia della definizione delle varie fattispecie incriminatrici, ha implementato la disciplina dei reati informatici soprattutto dal punto di vista processuale, ratificando una serie di norme della Convenzione di Budapest in merito alla raccolta di prove e indagini informatiche, tenendo conto delle esigenze di immodificabilità degli elementi di prova che per loro natura rischiano continuamente di essere alterati o resi inutili.

Nello specifico, in tema di ispezioni informatiche, con le modifiche aggiuntive all'art. 244 c.p.p., si è stabilito che l'autorità giudiziaria possa disporre

---

[238] Cfr. sul punto FATTA C., *Antiterrorismo e data retention*, in *Dir. inf. e informatica,* 2008, p. 403.

[239] ATERNO S., in ATERNO S., CORASANITI G., CORRIAS LUCENTE G., *L'attuazione della convenzione europea sul cybercrime, commento alla legge 18 marzo 2008 n. 48*, Padova, CEDAM, 2009, pp. 69 ss.

rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione[240]. Sotto il profilo della perquisizione cd. informatica, invece, la modifica ha interessato l'art. 247 c.p.p. al quale è stato aggiunto un nuovo comma 1-*bis*, il quale stabilisce che ove si ha motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, deve esserne disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. La disposizione "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" assume rilievo fondamentale, dal momento che prima della l. n. 48/2008 non veniva in alcun modo specificato in quale modo o secondo quali criteri potessero essere effettuate le perquisizioni[241].

Anche l'art. 254 c.p.p. in materia di sequestro di corrispondenza è stato modificato attraverso l'introduzione dell'art. 254-*bis* c.p.p. relativo alla possibilità di sequestrare dati informatici presso i fornitori di servizi informatici, telematici e di telecomunicazioni; è stata inserita inoltre una disposizione sul problema che concerne la custodia delle cose sequestrate (art. 259 comma 2 c.p.p.) e alcune garanzie circa il sequestro e la custodia di cose deperibili come appunto i dati informatici (modifica dell'art. 260 comma 2 c.p.p.)[242].

In materia di perquisizioni è stato modificato anche l'art. 352 c.p.p. per i casi di urgenza e di flagranza di reato: al comma 2, infatti, è stabilito che quando sussistono i presupposti e le altre condizioni previste, gli ufficiali di polizia giudiziaria possono adottare misure tecniche dirette ad assicurare la

---

[240] ATERNO S., *Digital Forensics (investigazioni informatiche)*, in *Dig. Disc. Pen.*, 2014, pp. 217 ss.

[241] *Ibid.*

[242] *Ibid.*

conservazione dei dati originali e ad impedirne l'alterazione; hanno inoltre facoltà di procedere con la perquisizione nel momento in cui c'è il fondato pericolo che le informazioni contenute nei dispositivi vengano cancellate o modificate[243].

L'art. 9 comma 3 l. n. 48 del 2008 ha integrato il comma 2 dell'art. 354 c.p.p., estendendo il potere della polizia giudiziaria di compiere accertamenti urgenti, finalizzati a conservare tracce e cose pertinenti al reato o ad evitare l'alterazione di luoghi e cose, ai dati, alle informazioni, ai programmi informatici e ai sistemi informatici o telematici. Secondo la norma, gli ufficiali di polizia devono adottare le misure tecniche per fare in modo che i dati si mantengano integri all'interno del sistema, effettuandone un duplicato attraverso una procedura che assicuri l'aderenza perfetta all'originale[244].

Infine, l'art. 248 c.p.p. relativo alla richiesta di consegna di dati, informazioni e programmi informatici, è stato modificato per evitare di risultare eccessivamente lesivo della privacy o invasivo nella sfera personale degli individui; in questo senso, l'Autorità Giudiziaria può richiedere al possessore del dispositivo di consegnare i dati o i file da analizzare, invece che procedere direttamente con la perquisizione[245].

4. *L'Unione Europea e la Decisione Quadro sugli attacchi informatici 2005/222 GAI*

Anche l'UE si è dimostrata estremamente prolifica in funzione della disciplina dei crimini informatici, soprattutto a seguito della Convenzione di Budapest, al fine di coordinare ed armonizzare l'azione degli Stati membri per una regolamentazione uniforme. Gli obiettivi perseguiti dall'UE in merito sono sostan-

[243] *Ibid*.

[244] *Ibid*.

[245] *Ibid*.

zialmente due: accrescere la consapevolezza dei principali rischi connessi alla *cybersecurity* e migliorare la preparazione e le capacità di risposta europee e nazionali a possibili attacchi o incidenti informatici[246]. In merito al primo dei due obiettivi, la Commissione europea incoraggia il dialogo fra Stati membri e istituzioni attraverso la creazione nel 2004 dell'Agenzia europea per la sicurezza delle reti e delle informazioni (ENISA, *European Network and Information Security Agency*), piattaforma per lo scambio di informazioni e *best practices* fra istituzioni UE, autorità nazionali e imprese, che fornisce inoltre pareri tecnici sia alle autorità degli Stato membri sia alle istituzioni comunitarie[247]. Nel corso degli anni, inoltre, si è proceduto con la stesura di una serie di risoluzioni non vincolanti in materia di *cybercrime*, come la Comunicazione della Commissione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo" del 28 Gennaio 2002 o la Comunicazione della Commissione "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica", che ha come scopo il raggiungimento di determinati obiettivi sull'accessibilità e l'affidabilità in Internet entro il 2020.

Tuttavia, il documento più meritevole di attenzione è certamente la Decisione Quadro 222/2005 GAI del Consiglio dell'Unione Europea "relativa agli attacchi contro i sistemi di informazione", con l'intento di proseguire i progetti portati avanti dalla Convenzione di Budapest, dando sempre maggior rilievo alla cooperazione fra gli Stati membri e lavorando sulla costituzione di una disciplina minima dei reati informatici, in modo tale da non appesantire il sistema giudiziario in materia di *cybercrime*.

La Decisione si occupa prevalentemente dei reati propriamente informatici, ossia accesso abusivo ai sistemi e danneggiamento informatico, e non vi

---

[246] FALLETTA P. MENSI M., *Il diritto del web. Casi e materiali*, Padova, CEDAM, 2015, p. 296.

[247] Regolamento CE n. 460/2004 del Parlamento europeo e del Consiglio del 10 Marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, in G.U.U.E. 13 Marzo 2004 n. L. 077.

sono disposizioni chiare o precise relativamente alla cooperazione internazionale. Si tratta dunque di uno strumento estremamente diverso dalla Convenzione, sia a livello di tematiche disposte all'interno che a livello di ampiezza dei contenuti (si tratta soltanto di 13 articoli, mentre la Convenzione ne conta 48), ma questa diversità va considerata come un lato positivo in quanto rende la Decisione un documento "complementare" per disciplinare la cooperazione fra gli Stati membri, che in questo caso non sono tenuti a ratificare il documento poiché l'obbligo sussiste già nel momento in cui entrano a far parte della Comunità[248].

L'art. 1 (*Definizioni*) della Decisione apre il documento copiando le definizioni di sistemi e di dati informatici dalla Convenzione di Budapest, aggiungendo la definizione del termine "senza diritto", che ricorrerà poi nei successivi articoli e che ha come significato la mancanza di autorizzazione per l'utilizzo del dispositivo (elemento che, in effetti, rappresenta già di per se stesso un abuso).

L'art. 2 (*Accesso illecito a sistemi di informazione*) descrive il reato a cui si riferisce e ne ammette la penalizzazione "almeno nei casi gravi", lasciando agli Stati la possibilità di decidere quando un caso sia definibile tale.

Gli artt. 3 (*Interferenza illecita per quanto riguarda i sistemi*) e 4 (*Interferenza illecita per quanto riguarda i dati*), sono relativi al reato di danneggiamento rispettivamente dei sistemi e dei dati, ma li definiscono come reati di "interferenza illecita", dicitura che rende la disciplina più flessibile e generica.

L'art. 5 (*Istigazione, favoreggiamento nonché complicità e tentativo*) riguarda le forme di manifestazione, simili in tutto e per tutto a quelle della Convenzione di Budapest, mentre gli artt. 6 (*Sanzioni*) e 7 (*Circostanze aggravanti*) trattano le forme di sanzione: oltre a ribadire i principi di effettività, proporzionalità e dissuasività da tenere sempre in considerazione nel momento in cui si applicano le sanzioni, si aggiunge nel secondo comma la trattazione

[248] Cfr. LANZIERI M., in *I reati informatici*, Milano, Altalex Editore, 2010, sul sito http://www.altalex.com/index.php?idnot=10897 (*La decisione quadro UE del 2005 sugli attacchi informatici*).

sulla durata della pena, che varia da uno a massimo tre anni. Sempre in merito alle sanzioni, inoltre, c'è da considerare un aspetto molto positivo della Decisione, che stabilisce nel Considerando n. 13 la non punibilità delle violazioni meno gravi, affinché si eviti una penalizzazione eccessiva. In Italia tale scelta dell'Unione Europea pare quasi non essere stata recepita: infatti analizzando la l. n. 547/1993 e anche la l. n. 48/2008 di ratifica alla Convenzione di Budapest non si rileva nessuna disposizione relativa ai reati di lieve entità, e anzi una penalizzazione e una tipizzazione dei reati a volte troppo severa[249].

Gli artt. 8 (*Responsabilità delle persone giuridiche*) e 9 (*Sanzioni applicabili alle persone giuridiche*) sono corrispondenti all'art. 12 della Convenzione, con la differenza che all'art. 9 vengono elencate non solo sanzioni di tipo pecuniario, ma anche sanzioni di tipo interdittivo, ossia esclusioni o divieti per le persone giuridiche che abbiano commesso il reato.

Gli artt. 10 (*Competenza giurisdizionale*) e 11 (*Scambio di informazioni*), infine, sono relativi al rapporto e al coordinamento fra Stati, stabilendo dei criteri per la scelta della giurisdizione e invitando gli Stati a servirsi dei punti di contatto per lo scambio di informazioni. Questi due articoli risultano innovativi rispetto a quelli della Convenzione di Budapest, poiché dal punto di vista della giurisdizione la Decisione fa riferimento agli stessi criteri definiti all'interno della Convenzione, il collegamento territoriale oppure la nazionalità d'autore, ma aggiunge ulteriori dettagli, specificando che la giurisdizione dello Stato deve essere prevista in almeno due situazioni, ossia nel caso l'autore del reato abbia commesso la fattispecie mentre era fisicamente presente all'interno del territorio a prescindere da dove si trovasse il sistema attaccato, oppure nel caso in cui sia il sistema attaccato ad essere presente all'interno del territorio a prescindere da dove si trovasse l'autore del reato. Inoltre, la Decisione non solo invita gli Stati a cooperare al fine di ricercare insieme la soluzione a possibili contrasti giurisdizionali, ma suggerisce anche

[249] LANZIERI M., *I reati informatici*, Altalex Editore, Milano, 2010 su http://www.altalex.-com/index.php?idnot=10897 (*La decisione quadro UE del 2005 sugli attacchi informatici*).

delle linee guida per risolvere il problema, prima fra tutte la possibile contrazione dei procedimenti in un unico Paese per evitare lo spostamento eccessivo delle prove che potrebbe portare ad una dispersione.

5. Recenti iniziative sovranazionali in materia di cybersecurity

L'emanazione della Decisione Quadro 222/2005 GAI ha ulteriormente implementato la proliferazione di atti di varia natura in merito alla necessità per l'Europa di disciplinare in maniera univoca e coerente i crimini informatici e stabilire i principi di cooperazione internazionale.

Fra le più significative, sono da menzionare la direttiva 114/2008 EC in merito alle "infrastrutture critiche europee"[250], nella quale venivano individuati i network che potessero essere soggetti a rischi e si stabilivano piani di sicurezza da attuare, e la strategia elaborata dalla Commissione Europea nel Febbraio 2013 sulla sicurezza informatica, dal titolo "Uno spazio informatico aperto e sicuro". La strategia evidenzia cinque priorità di cui tenere conto per assicurare una maggiore sicurezza informatica: conseguire la resistenza dei sistemi informatici; ridurre drasticamente la criminalità informatica; sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune; sviluppare le risorse industriali e tecnologiche per la sicurezza informatica; istituire una coerente politica internazionale del cyberspazio per l'Unione Europea e sostenere i valori fondamentali dell'UE[251].

Un testo di grande rilievo, poi, rimane la direttiva 40/2013 UE sugli attacchi contro i sistemi di informazione del Parlamento europeo e del Consi-

---

[250] Direttiva 114/2008 CE del Consiglio dell'8 Dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, in G.U.C.E 23 Dicembre 2008 n. L. 435. Tale strumento normativo è stato recepito in Italia con il d.lgs. 11 Aprile 2011, n. 61, in G.U., n. 102 del 4 Maggio 2011.

[251] FALLETTA P., MENSI M., *cit*. p. 297.

glio, che sostituisce la decisione 222/2005 GAI[252]. La direttiva dà indicazioni in merito ai reati propriamente informatici, ossia l'accesso abusivo, il danneggiamento di dati o sistemi e l'intercettazione, stabilendo poi le relative sanzioni ed i profili di responsabilità, nonché i principi per un miglioramento della cooperazione fra Stati, fra pubblico e privati, e fra forze speciali relative alla sicurezza sulla Rete. Ulteriore introduzione è una norma sulla giurisdizione, che rende responsabile lo Stato sul cui territorio è commesso il reato o del quale è cittadino l'autore dell'illecito; la disposizione aggiunge inoltre la responsabilità di uno Stato qualora l'autore dell'illecito sia fisicamente presente su quel territorio, oppure che sia presente fisicamente il dispositivo attaccato, e anche nel caso in cui l'autore risieda sul territorio del suddetto Stato nel momento del compimento dell'illecito o nel caso sul territorio abbia sede la persona giuridica che trae vantaggio dall'illecito[253].

Altra recente Direttiva da tenere in considerazione è quella relativa alla Network and Information Security (NIS). Approvata dal Parlamento europeo a Marzo del 2014, si pone come obiettivo una maggiore difesa del cyberspazio sia all'interno dei singoli Stati, sia mettendo in atto una difesa comune ed elaborando principi di politica internazionale per agire in maniera coordinata. La direttiva si rivolge anche ai privati e ai market operators, che devono adottare le corrette misure per garantire una protezione dai rischi e la sicurezza delle reti. Devono inoltre notificare alla competente autorità nazionale il verificarsi di incidenti, definiti all'interno della direttiva come "qualsiasi circostanza o evento che ha un effetto negativo sulla sicurezza"[254].

---

[252] ENISA, *The Directive on attacks against information systems. A Good Practice Collection for the implementation and application of this Directive*, http://www.coe.int/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/Presentations/Workshop1/Jo_De_Muynck-ENISA-Octopus.pdf .

[253] Cfr. art. 12 Direttiva 40/2013 UE.

[254] Art. 14 NIS.

Infine è da segnalare l'istituzione, nel 2013, del Centro Europeo per la lotta alla criminalità informatica (EC3), con il compito di integrare gli interventi legislativi con attività operative sui sistemi informatici.

Conclusioni

A conclusione del lavoro di analisi del panorama dei crimini informatici e delle norme che li regolano a livello nazionale e sovranazionale, sono svariate le conclusioni, ma anche le domande, alle quali si giunge.

Il primo elemento che va preso in considerazione è la continua evoluzione sia delle tecnologie informatiche, sia dei reati che abusano del progresso, sia delle discipline che sono tenute a regolare e ad impedire la crescita di tali abusi. Infatti, con il passare del tempo il progresso tecnologico avanza in maniera esponenziale, e si vanno via via presentando nuovi strumenti materiali ed immateriali che migliorano la vita di ogni giorno ma soprattutto entrano a far parte della quotidianità e della vita sociale, culturale, economica e amministrativa dei Paesi. Esattamente alla stessa velocità proliferano i crimini perpetrati attraverso i dispositivi informatici e sul Web: crimini nuovi, strettamente legati all'utilizzo dei sistemi, o crimini tradizionali che trovano nelle nuove tecnologie ulteriori prospettive di azione. Le figure dei criminali, allo stesso modo, aumentano continuamente, poiché diventa sempre più semplice acquisire le capacità per commettere reati attraverso i computer e la rete, e al contempo aumentano i metodi per eludere le misure di sicurezza.

Al continuo aggiornamento delle tecnologie e dei crimini ad esse correlati dovrebbe corrispondere un equivalente e costante aggiornamento della produzione normativa che disciplini le fattispecie di reati informatici che vanno configurandosi; purtroppo questa aspettativa rimane il più delle volte delusa, a causa della difficoltà oggettiva di stare al passo con l'implemento costante delle tecnologie, nel momento in cui l'ema-

nazione di norme si realizza dopo un processo lungo e complesso che ne rallenta la produzione. Tuttavia, soprattutto negli ultimi anni anche nel nostro Paese ha concentrato la propria attenzione sul tema della sicurezza attraverso una serie di Relazioni che il Governo ha presentato al Parlamento, sulla politica dell'informazione per la sicurezza. In tali atti la minaccia cibernetica viene presentata come "la sfida più impegnativa per il sistema Paese"[255], ed è un segnale di come il Paese stia affrontando con consapevolezza il problema della minaccia cibernetica. Altro elemento importante è rappresentato dal decreto del 24 Gennaio 2013 del Presidente del Consiglio[256] in merito al rafforzamento dello spazio cibernetico italiano, indirizzando gli attori pubblici e privati a mettere in atto i giusti provvedimenti per la sicurezza e la protezione dei sistemi nel loro complesso. Il decreto ha stabilito la divisione dei compiti degli attori politici ed amministrativi per coordinare le attività, e ha rafforzato la cooperazione fra i vari settori della vita pubblica affinché si elaborino degli efficaci meccanismi di difesa.

Dunque, molto è stato fatto, molto si sta facendo, ma ancora molto altro è da fare. Questo perché fin troppo spesso affiorano incertezze interpretative da parte della giurisprudenza in merito alle disposizioni che disciplinano il fenomeno dei crimini informatici, introdotte in Italia dalla l. n. 547/1993 e in alcuni casi modificate dopo la l. n. 48/2008. Infatti dall'analisi emerge una certa disattenzione del legislatore, che potrebbe aver agito in maniera eccessivamente superficiale per rispondere in

[255] Governo italiano, *Relazione sulla politica dell'informazione per la sicurezza*, 2013, pp. 37-47.

[256] D.P.C.M., 24 Gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, in G.U. Serie Generale n. 66 del 19 Marzo 2013.

modo rapido alla necessità di un quadro normativo, trascurando tuttavia aspetti che avrebbero permesso una maggiore chiarezza nell'interpretazione. Questa conclusione è frutto del lavoro di analisi in base alle indicazioni della dottrina, che non risulta quasi mai concorde nel dare un senso ai dettami del legislatore.

Anche a livello sovranazionale tanti passi si stanno compiendo verso una maggiore difesa dello spazio cibernetico, facendo leva soprattutto sulla necessità di cooperazione e coordinazione sia dal punto di vista investigativo che da quello giuridico. Questo aspetto è essenziale in ragione dei caratteri tipici, già evidenziati, dei crimini informatici e anche del bisogno di armonizzazione delle norme in una società quanto mai globalizzata.

Tuttavia, ci sono una serie di problemi che ancora vedono la soluzione piuttosto lontana. Due su tutti: la questione del bilanciamento fra tutela delle informazioni e tutela della libertà personale e, connesso a questo, il problema della cd. *data retention*, della conservazione in rete dei dati che potrebbero agevolare le indagini ma che fanno parte della sfera privata degli individui. Questi ambiti sono particolarmente delicati poiché è necessario adottare comportamenti che non implichino una lesione dei diritti fondamentali ma che al contempo siano efficaci al fine della protezione dei sistemi: l'equilibrio, in questo senso, è difficile da raggiungere e ancor più difficile da mantenere.

Infine, ultimo aspetto che a mio parere va tenuto fortemente in considerazione pur non essendo strettamente giuridico, è il tema della

consapevolezza in merito ai crimini informatici, al loro dilagare e alla loro centralità nella vita quotidiana. Troppo spesso, tale consapevolezza manca fra i fruitori dei sistemi informatici, poco aggiornati in merito ai rischi che si corrono lavorando con i dispositivi e navigando in rete. Tale consapevolezza è necessaria anche per una conseguente conoscenza delle destinazioni delle informazioni personali che si depositano in rete o all'interno dei sistemi informatici. Si sente fortemente la necessità di realizzare quanto i reati informatici siano quanto mai reali, oggi che le tecnologie informatiche sono parte della nostra vita e che vanno aggiornandosi continuamente. Solo partendo dal basso, con un'informazione migliorata ai soggetti che ogni giorno utilizzano e, in taluni casi, dipendono da queste tecnologie, si potrà sperare in un miglioramento della sicurezza e in una più consapevole fruizione dei vantaggi che derivano dal progresso tecnologico.

Bibliografia

AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni*. Matelica, Halley, 2006

ANTOLISEI F., *Manuale di diritto penale. Leggi complementari : 2: Reati fallimentari, reati ed illeciti amministrativi in materia tributaria, di lavoro, ambientale ed urbanistica, responsabilità degli enti*. 13. Ed. a cura di C. F. Grosso. – Milano, Giuffrè, 2014

ATERNO S., CORASANITI G., CORRIAS LUCENTE G., *L'attuazione della convenzione europea sul cybercrime , commento alla legge 18 marzo 2008 n. 48*. Padova, CEDAM, 2009

ATERNO S., *Digital Forensics (investigazioni informatiche)*, in "Digesto delle discipline penalistiche", 2014

ATTANASIO A., COSTABILE G. *IISFA Memberbook 2012 Digital Forensics : condivisione della conoscenza tra i membri dell'Iisfa Italian Chapter.* Forlì, Experta, 2013

BALKIN J. M., *Cybercrime : digital cops in a networked environment*. New York, N. Y.University Press, 2007

BARBAGLI M. GATTI U., *La criminalità in Italia*. Bologna, Il Mulino, 2002

BERGHELLA F. - BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in "Cassazione penale", 1995

BETZU M., *Regolare Internet. La libertà di informazione e di comunicazione nell'era digitale*. Torino, Giappichelli, 2012

BORRUSO V.R., BUONOMO G., CORASANITI G., D'AIETTI G., *Profili penali dell'informatica*. Milano, Giuffrè, 1994

CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*. Milano, Giuffrè, 2008

CAJANI F., COSTABILE G., *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*. Forlì, Experta, 2012

CASEY E., BRENNER S. *Digital Evidence and Computer Crime : forensic science, computers, and the Internet*. Waltham, MA Academic Press, 2011

CLIFFORD R.D., *Cybercrime: the investigation, prosecution and defense of a computer related crime*. Carolina Academic Press, 2001

CLOUGH J., *Principles of Cybercrime*, Cambridge University Press, 2015

COLOMBO E., La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali, in "Ciberspazio e diritto", 2009

CORASANITI G., CORRIAS LUCENTE, G., ATERNO S., *Cybercrime, responsabilità degli enti e prova digitale : commento alla Legge 18 marzo 2008, n. 48 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*. Padova, CEDAM, 2009

CORRIAS LUCENTE G., *Informatica e diritto penale. Elementi per una comparazione del diritto statunitense*, in "Diritto dell'informazione e dell'informatica", 1987

COUNCIL OF EUROPE, *Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-related Crime* (Sept. 13, 1989)

COUNCIL OF EUROPE / COMMITTEE OF MINISTERS, *Recommendation No. R (95) 13 Concerning Problems of Criminal Procedural Law connected with Information Technology*, (Sept. 11, 1995)

CREMONESI C., MARTELLA G., *I crimini informatici : storia, tecniche e difese*. Milano, Mondadori Informatica, 1990

D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*. Milano, Giuffrè, 2012

DELFINI F., FINOCCHIARO G., *Diritto dell'informatica*. San Mauro Torinese, UTET giuridica, 2014

DESTITO V., v. *Reati Informatici*, in "Digesto delle discipline penalistiche" Aggiornamento : A-Z. Torino, UTET, 2010

DOLCINI E., MARINUCCI G., *Commento all'art. 615-quater c.p.*, in *Codice penale commentato,* Milano, Ipsoa, 2006

FALLETTA P., MENSI M., *Il diritto del Web. Casi e materiali*. Padova, CEDAM, 2015

FANELLI A., *Telefonate abusive e frode informatica*, in "Foro italiano", III, 1999

FATTA C., *Antiterrorismo e data retention*, in "Diritto dell'informazione e informatica", 2008

FIANDACA G., MUSCO E., *Diritto penale. Parte speciale*. Vol. II, Bologna, Zanichelli, 1996

FIANDACA G., MUSCO E., *Diritto penale. Parte speciale. 2.1: I delitti contro la persona*. Bologna, Zanichelli, 2013

FLOR R., *Identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in "Rivista italiana di diritto e procedura penale", 2007.

FLOR R., *Art. 615-ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in "Diritto penale processuale", 2008

FONDAROLI D., SOLA L., *La nuova normativa in materia di criminalità informatica: alcune riflessioni*. Bologna, Clueb, 1995

FROSINI V., *La criminalità informatica*, in "Diritto dell'informazione e informatica", 1997

IASELLI M., MAGGIPINTO A., (a cura di), *Sicurezza e anonimato in Rete. Profili giuridici e tecnologici della navigazione anonima*. Milano, Nyberg, 2005

ILARDA G., MARULLO G., *Cybercrime. Conferenza internazionale: la Convenzione del Consiglio d'Europa sulla criminalità informatica*. Milano, Giuffrè, 2004

LORUSSO P., *L'insicurezza dell'era digitale. Tra cybercrimes e nuove frontiere dell'investigazione: Tra cybercrimes e nuove frontiere dell'investigazione*. Milano, FrancoAngeli, 2011

LUPARIA L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa (l.18 Marzo 2008, n. 48). Profili processuali*, in "Diritto penale processuale", 2008.

LUPARIA L., *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime (l.18 Marzo 2008, n. 48)*, Milano, Giuffrè, 2009

LUSITANO D., *In tema di accesso abusivo ai sistemi informatici o telematici*, in "Giurisprudenza italiana", 1998

MANTOVANI M., *Brevi note a proposito della nuova legge sulla criminalità informatica*, in "Critica del diritto", 1994

MANTOVANI M., *Diritto Penale. Parte speciale. Delitti contro la persona*. Padova, CEDAM, 2008

MANTOVANI M., *Diritto penale. Parte speciale. Delitti contro il patrimonio*. Padova, CEDAM, 2009

MENGONI E., *Accesso autorizzato al sistema informatico o telematico e finalità illecite: nuovo round alla configurabilità del reato[Nota a sentenza] Sez. V, 16/2/2010 (dep. 21/5/2010),* in "Cassazione penale", 2011

MERLI A., *Il diritto penale dell'informatica: legislazione vigente e prospettive di riforma*, in "Giustizia penale", 1993

MOORE R., *Cybercrime: investigative high-technology computer crime*, LexisNexis Publication, 2005

MUCCIARELLI F., *voce Computer (disciplina giuridica del) nel diritto penale*, in "Digesto delle discipline penalistiche" Torino, UTET, 1990

MUCCIARELLI F., *Commento all'art. 4 della l. 547/1993*, in "Legislazione penale", 1996

MUCCIARELLI F., *Commento all'art. 10 della l. 547/1993*, in "Legislazione penale", 1996

NERI G., *Criminologia e reati informatici. Profili di diritto penale dell'economia*. Napoli, Jovene, 2014

NORRIS P., *The Worldwide Digital Divide: Information Poverty, the Internet and Development*, Cambridge, John F. Kennedy School of Government Harvard University, 2000

PADOVANI T. (a cura di), *Codice Penale*. Milano, Giuffré, 2007

PAIS S. - PERROTTA G., *L'indagine investigativa. Manuale teorico-pratico*, Padova, Primiceri, 2015

PAGLIARO A., *Principi di diritto penale. Parte speciale. 3: Delitti contro il patrimonio*. Milano, Giuffrè, 2003

PARKER D.B., *Crime by Computer*. New York, Charles Scribsen's Sons, 1976

PECORELLA C., sub *art. 617-sexies*, in *Commento all'art. 615-quater, c.p.,* in DOLCINI E., MARINUCCI G. (a cura di), *Codice penale commentato,* Milano, Giuffrè, 2004

PECORELLA C., *Diritto penale dell'informatica*. Padova, CEDAM, 2006

PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in "Ciberspazio e diritto", 2008

PICA G., *La disciplina penale degli illeciti in materia di tecnologie informatiche e telematiche*, in "Rivista penale dell'economia", 1995

PICA G., *Reati informatici e telematici*, in "Digesto delle discipline penalistiche" Aggiornamento : A-Z. Torino, UTET, 2000

PICOTTI L., *La rilevanza penale degli atti di "sabotaggio" ad impianti di elaborazione dati*, in "Diritto dell'informazione e dell'informatica", 1986

PICOTTI L., *Commento all'art. 5 della l.547/1993*, in "Legislazione penale", 1996

PICOTTI L. RINALDI R., *Commento all'art. 6 della legge 547 del 1993*, in "Legislazione penale", 1996

PICOTTI L. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*. Padova, CEDAM, 2004

PICOTTI L., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in "Il diritto penale del futuro",, 2006

PICOTTI L., *La ratifica della Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*. Padova, CEDAM, 2008

PICOTTI L., *La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee*, in "Rivista trimestrale di diritto penale dell'economia", 2011

PICCINI M.L., VACIAGO G., *Computer crime: casi pratici e metodologie investigative dei reati informatici*, Bergamo, Moretti&Vitali, 2008

RICHARDS J., *Transnational criminal organizations, Cybercrime and money laundering*, CRC Press, Boca Raton, FL, 1999

RINALDI P.G., *Commento all'art. 6 della l. 547/1993*, in "Legislazione penale", 1996

ROSSI VANNINI A., *La criminalità informatica: le tipologie di computer crimes di cui alla l. 547/1993 dirette alla tutela della riservatezza e del segreto*, in "Rivista trimestrale di diritto penale dell'economia", 1994

SALVADORI I., *Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive "de iure condendo"*, in "Ciberspazio e diritto", 2008

SARZANA C., IPPOLITO S., *Informatica, Internet e diritto penale*. Milano, Giuffrè, 2010

SIEBER U., *The international handbook for computer crime. Computer-Related Economic Crime and the Infringements of Privacy*. New York, John Wiley & Sons, 1986

SIEBER U., *Responsabilità penali per la circolazione di dati nelle reti internazionali di computer*, in "Rivista trimestrale di diritto penale dell'economia", 1997

SIEBER U., *Organised crime in Europe: the threat of cybercrime. Situation Report 2004*. Strasburgo, Council of Europe Publishing, 2005

SMITH R.G., GRABOSKY P., URBAS G., *Cyber criminals on trial*, Cambridge University Press, 2004

STILO L., *Indebito utilizzo di carte di credito su Internet*, in "Nuovo diritto", 2003

TAPPERO MERLO G., *Soggetti e ambiti della minaccia cibernetica: dal sistema paese alle proposte di cyber governance?* in "La comunità internazionale : rivista trimestrale della Società italiana per l'organizzazione internazionale", 2012

VACIAGO G., *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*. Torino, Giappichelli, 2012

VALVO A., *Diritti umani e realtà virtuale. Normativa europea e internazionale*. Firenze, Amon, 2013

ZICCARDI G., *I virus informatici: aspetti tecnici e giuridici, in* "Ciberspazio e diritto", 2001

Giurisprudenza

1282 (Cass. Pen., Sez. Un., 13 Dicembre 1996)

5937 (Cass. Pen., sez. III, 11 Febbraio 2000)

12732 (Cass. Pen., sez. V, 6 Dicembre 2000)

4576 (Cass. Pen., V sez., 24 Novembre 2003)

1823 (Trib. Bologna, 21 Luglio 2005)

369 (Cass. Pen., sez. III, 27 Marzo 2008)

1727 (Cass. Pen., sez. V, 16 Gennaio 2009)

243602 (Cass. Pen., sez. V, 13 Febbraio 2009)

1934 (Cass. Pen., sez. V, 21 Gennaio 2011)

17325 (Cass., Sez. Un., 26 marzo 2015)

Riassunto

I crimini informatici sono fenomeni in continua crescita; ciò in ragione del fatto che il rischio associato alla commissione del reato è basso se paragonato agli alti guadagni che ne derivano. Per questa ragione le informazioni trasmesse online sono considerate alla stregua di materie prime essenziali per il funzionamento di una nazione e il suo successo nell'area internazionale; si tratta di "un complesso di informazioni su progetti, brevetti, piani strategici e quant'altro messo in una Rete che, anche se garantita dal muri digitali di protezione è, a quanto sembra, ancora troppo vulnerabile. Infatti, a rischiare attacchi cibernetici sono proprio i paesi a maggior dotazione di *know how*, innovativo e con alta esposizione in Rete. E' la doppia faccia di Internet e dei vantaggi che offre l'innovazione dei sistemi ICT […]".

Il pericolo maggiore degli attacchi cibernetici è costituito forse dalle due caratteristiche principali di questa tipologia di attacchi. La prima di esse è la cd. asimmetria degli attacchi, ossia la possibilità per chi colpisce di farlo in maniera assolutamente anonima, rapidissima e ad una grande distanza rispetto al dispositivo attaccato poiché, spesso, è necessaria la presenza di una rete Internet; la seconda caratteristica invece è costituita dalla potenziale semplicità degli attacchi, che sono diventati soprattutto negli ultimi anni accessibili anche ad individui non dotati di particolari capacità tecniche.

La difesa dello spazio cibernetico diventa ogni giorno più essenziale per prevenire i rischi di attacco e garantire una sicurezza che ogni giorno di più si dimostra fondamentale per i singoli Paesi. L'*International Telecommunication Union* (ITU) delle Nazioni Unite definisce la *cybersecurity* come "l'insieme di strumenti, interventi, concetti, linee guida, impostazioni della gestione del rischio, azioni pratiche, procedute e tecnologie che possono essere utilizzate per proteggere lo spazio e la struttu-

ra cibernetica e i loro utilizzatori". In altri termini, la *cybersecurity* è considerata il contesto in cui cercare soluzioni ed elaborare strategie combinate al fine di difendere lo spazio cibernetico dalle minacce sia a livello nazionale sia transnazionale, dato il carattere spiccatamente globale della minaccia.

Oggetto dello studio è la ricognizione delle tipologie di crimini informatici nate nel corso degli anni all'interno della quale si prevede di analizzare le risposte normative a questi reati, sia dal punto di vista dell'ordinamento interno che da quello della cooperazione internazionale, attraverso l'esame della disciplina del legislatore e delle istituzioni sovranazionali.

Il primo pensiero che soggiunge nel momento in cui si parla di reati informatici è che si tratti di un argomento piuttosto recente, e di conseguenza recentemente disciplinato. Sorprende invece scoprire che la legge a cui si fa riferimento *in primis* nel caso dei crimini informatici è la l. n. 547/1993, una legge che quindi ha 23 anni ma che ancora risulta fumosa nei suoi contenuti: infatti, a tutt'oggi risulta a volte difficile comprendere su quali reati volesse andare ad agire il legislatore. Infatti, la l. n. 547/1993 ha introdotto alcune disposizioni volte ad incriminare i reati informatici ed alcune di esse sono state successivamente modificate a seguito della ratifica italiana alla Convenzione di Budapest sul *Cybercrime* (23 Novembre 2001), attraverso la l. n. 48/2008.

Diventa necessario dunque acquisire una maggiore consapevolezza in merito ai rischi che si corrono nel momento in cui si decide di utilizzare i sistemi informatici e le nuove tecnologie che fanno oggi parte della nostra quotidianità in ogni ambito, dall'economia alla pubblica amministrazione ma anche semplicemente nella vita privata degli individui, che spesso sono all'oscuro dei pericoli che si nascondono specialmente all'interno della rete. È fondamentale comprendere il corretto funzionamento

di tali tecnologie, i rischi che si corrono e le potenziali condotte illegali realizzabili con esse.

I reati informatici sono convenzionalmente denominati *cybercrimes* poiché presentano come elemento comune l'uso di dispositivi elettronici. L'influenza della cd. *information technology* sulla commissione e percezione dell'illecito non è spiegabile attraverso i tradizionali canoni e approcci delle scienze criminologiche. Tuttavia, definire in modo puntuale i *cybercrimes* non è semplice poiché questo termine include al proprio interno una serie di condotte illecite molto diverse fra loro, di varia natura, tutte unite dal denominatore comune che è l'utilizzo di un computer o di un dispositivo informatico.

Per quanto concerne il contesto italiano, il legislatore è intervenuto attraverso la l. n. 547/1993 su settori estremamente eterogenei, che possono essere raggruppati in quattro grandi macro-categorie: le frodi informatiche, le falsificazioni, la lesione dell'integrità dei dati e dei sistemi e violazione della riservatezza di comunicazioni informatiche.

Le frodi informatiche sono disciplinate all'art. 640-*ter* c.p., che possono essere assimilate al reato di truffa per quanto riguarda il profilo dell'oggettività ma che tuttavia sono si caratterizzano per l'utilizzo di dispositivi informatici e quindi per l'assenza di un effettivo comportamento illecito di un essere umano, quanto piuttosto l'azione di una macchina, azione diretta a procurarsi un ingiusto profitto attraverso l'altrui danno; le cd. truffe online sono un esempio emblematico di questa fattispecie di reato.

Le falsificazioni documentali sono disciplinate ai sensi dell'art. 491-*bis* c.p. nel quale si è tentata una sostanziale equiparazione fra la falsificazione di documenti informatici e quella di documenti cartacei (pubblici o privati) purché abbiano una qual-

che valenza probatoria. L'art. 491-*bis* c.p., inoltre, prima della modifica effettuata con l'emanazione della l. n. 48/2008, conteneva al proprio interno anche la definizione di documento informatico, ossia "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli". Per ciò che concerne invece la falsificazione del contenuto di comunicazioni informatiche, è disciplinato all'art. 617-*sexies* c.p. ed anche in questo caso la disciplina è la stessa che per la fattispecie di falsificazione del contenuto di comunicazioni telefoniche o telegrafiche, ossia che possono essere pubbliche o private purché la comunicazione falsificata venga in qualche modo utilizzata.

In merito alla lesione dell'integrità dei dati e dei sistemi informatici, in questo caso l'assimilazione al reato tradizionale di lesione dell'integrità della "cosa mobile" (disciplinato all'art. 635 c.p.) risultava piuttosto forzata in quanto il *software* non poteva far parte della categoria di "cose" definita precedentemente dalla disciplina del reato tradizionale. Per questa ragione sono stati aggiunti gli artt. 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies*, ma sono anche state modificate disposizioni preesistenti, come l'art. 392 c.p. relativo alla "violenza sulle cose" e l'art. 420 c.p. in merito agli attentati ad impianti di pubblica utilità, aggiungendo anche la condotta di attentato a sistemi informatici contenenti dati, informazioni o programmi; la modifica successiva all'emanazione della l. n. 48/2008 ha però abrogato i commi aggiunti con la l. n. 547/1993.

Infine, per ciò che concerne la violazione della riservatezza di comunicazioni informatiche, il legislatore ha incriminato la condotta di accesso abusivo ad un sistema informatico o telematico all'art. 615-*ter* c.p., di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, ma ha anche ampliato l'ambito di operatività dell'art. 621 c.p. in merito alla rivelazione del contenuto di documenti segreti, comprendendo anche quelli presenti su dispositivi informatici. Inoltre, sono state aggiunte ulteriori fattispecie di reato all'art. 617-*quater* c.p., in merito alle figure di

intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche, e all'art. 617-*quinquies* c.p. in merito all'installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche.

Nell'ambito dei reati informatici, tuttavia, è fondamentale tenere in considerazione anche il contesto internazionale, poiché il concetto di prevenzione e disciplina dei reati informatici, per definizione, non può prescindere da una coordinazione sovranazionale, dal momento che il reato informatico ha carattere puramente virtuale e spesso distaccato da una qualsiasi connotazione fisica interna ad uno Stato; per questa ragione, si è rivelata necessaria una continua cooperazione internazionale per la lotta a questi reati.

Sebbene la Convenzione di Budapest sul *Cybercrime* del 2001 rappresenti indubbiamente la fonte più completa in merito, una vera e propria rivoluzione nel panorama europeo in materia di reati informatici poiché si tratta della prima fonte pattizia di norme che disciplinassero questo nuovo tipo di reati, i primi tentativi di regolamentazione cominciano ad affacciarsi già diverso tempo prima: si pensi che già nel 1976 si tenne a Strasburgo la prima Conferenza del Consiglio d'Europa sugli aspetti criminologici dei reati economici, nel corso della quale vennero trattati anche gli illeciti compiuti attraverso dispositivi informatici, seppure in maniera generica. Tutti questi atti, però, sono configurabili come fonti di *soft law*, che non ponevano in effetti alcun tipo di obbligo specifico per quanto riguardasse la disciplina dei crimini informatici, lasciando comunque libera azione ai singoli legislatori dei vari Stati e non ponendo attenzione all'elemento della cooperazione secondo una base legislativa comune sia dal punto di vista sostanziale che da quello procedurale.

Anche l'UE si è dimostrata estremamente prolifica in funzione della disciplina dei crimini informatici, soprattutto a seguito della Convenzione di Budapest, al fine di coordinare ed armonizzare l'azione degli Stati membri per una regolamentazione uni-

forme. Gli obiettivi perseguiti dall'UE in merito sono sostanzialmente due: accrescere la consapevolezza dei principali rischi connessi alla *cybersecurity* e migliorare la preparazione e le capacità di risposta europee e nazionali a possibili attacchi o incidenti informatici. In merito al primo dei due obiettivi, la Commissione europea incoraggia il dialogo fra Stati membri e istituzioni attraverso la creazione nel 2004 dell'Agenzia europea per la sicurezza delle reti e delle informazioni (ENISA, *European Network and Information Security Agency*), piattaforma per lo scambio di informazioni e *best practices* fra istituzioni UE, autorità nazionali e imprese, che fornisce inoltre pareri tecnici sia alle autorità degli Stato membri sia alle istituzioni comunitarie. Nel corso degli anni, inoltre, si è proceduto con la stesura di una serie di risoluzioni non vincolanti in materia di *cybercrime*, come la Comunicazione della Commissione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo" del 28 Gennaio 2002 o la Comunicazione della Commissione "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica", che ha come scopo il raggiungimento di determinati obiettivi sull'accessibilità e l'affidabilità in Internet entro il 2020.

Tuttavia, il documento più meritevole di attenzione è certamente la Decisione Quadro 222/2005 GAI del Consiglio dell'Unione Europea "relativa agli attacchi contro i sistemi di informazione", con l'intento di proseguire i progetti portati avanti dalla Convenzione di Budapest, dando sempre maggior rilievo alla cooperazione fra gli Stati membri e lavorando sulla costituzione di una disciplina minima dei reati informatici, in modo tale da non appesantire il sistema giudiziario in materia di *cybercrime*.

L'emanazione della Decisione Quadro 222/2005 GAI ha ulteriormente implementato la proliferazione di atti di varia natura in merito alla necessità per l'Europa di

disciplinare in maniera univoca e coerente i crimini informatici e stabilire i principi di cooperazione internazionale.

Fra le più significative, sono da menzionare la direttiva 114/2008 EC in merito alle "infrastrutture critiche europee", nella quale venivano individuati i *network* che potessero essere soggetti a rischi e si stabilivano piani di sicurezza da attuare, e la strategia elaborata dalla Commissione Europea nel Febbraio 2013 sulla sicurezza informatica, dal titolo "Uno spazio informatico aperto e sicuro".

Un testo di grande rilievo, poi, rimane la direttiva 40/2013 UE sugli attacchi contro i sistemi di informazione del Parlamento europeo e del Consiglio, che sostituisce la decisione 222/2005 GAI.

Altra recente direttiva da tenere in considerazione è quella relativa alla *Network and Information Security* (NIS). Approvata dal Parlamento europeo a Marzo del 2014, si pone come obiettivo una maggiore difesa del cyberspazio sia all'interno dei singoli Stati, sia mettendo in atto una difesa comune ed elaborando principi di politica internazionale per agire in maniera coordinata. La direttiva si rivolge anche ai privati e ai *market operators*, che devono adottare le corrette misure per garantire una protezione dai rischi e la sicurezza delle reti. Devono inoltre notificare alla competente autorità nazionale il verificarsi di incidenti, definiti all'interno della direttiva come "qualsiasi circostanza o evento che ha un effetto negativo sulla sicurezza".

Infine è da segnalare l'istituzione, nel 2013, del Centro Europeo per la lotta alla criminalità informatica (EC3), con il compito di integrare gli interventi legislativi con attività operative sui sistemi informatici.

A conclusione del lavoro di analisi del panorama dei crimini informatici e delle norme che li regolano a livello nazionale e sovranazionale, sono svariate le conclusioni, ma anche le domande, alle quali si giunge.

Il primo elemento che va preso in considerazione è la continua evoluzione sia delle tecnologie informatiche, sia dei reati che abusano del progresso, sia delle discipline che sono tenute a regolare e ad impedire la crescita di tali abusi. Infatti, con il passare del tempo il progresso tecnologico avanza in maniera esponenziale, e si vanno via via presentando nuovi strumenti materiali ed immateriali che migliorano la vita di ogni giorno ma soprattutto entrano a far parte della quotidianità e della vita sociale, culturale, economica e amministrativa dei Paesi. Esattamente alla stessa velocità proliferano i crimini perpetrati attraverso i dispositivi informatici e sul Web: crimini nuovi, strettamente legati all'utilizzo dei sistemi, o crimini tradizionali che trovano nelle nuove tecnologie ulteriori prospettive di azione. Le figure dei criminali, allo stesso modo, aumentano continuamente, poiché diventa sempre più semplice acquisire le capacità per commettere reati attraverso i computer e la rete, e al contempo aumentano i metodi per eludere le misure di sicurezza.

Al continuo aggiornamento delle tecnologie e dei crimini ad esse correlati dovrebbe corrispondere un equivalente e costante aggiornamento della produzione normativa che disciplini le fattispecie di reati informatici che vanno configurandosi; purtroppo questa aspettativa rimane il più delle volte delusa, a causa della difficoltà oggettiva di stare al passo con l'implemento costante delle tecnologie, nel momento in cui l'emanazione di norme si realizza dopo un processo lungo e complesso che ne rallenta la produzione. Tuttavia, soprattutto negli ultimi anni anche nel nostro Paese ha concentrato la propria attenzione sul tema della sicurezza attraverso una serie di Relazioni che il Governo ha presentato al Parlamento, sulla politica dell'informazione per la sicurezza. In tali atti la minaccia cibernetica viene presentata come "la sfida più impegnativa per il sistema Paese", ed è un segnale di come il Paese stia affrontando con consapevolezza il problema della minaccia cibernetica. Altro elemento importante è rappresentato dal decreto del 24 Gennaio 2013 del Presidente del Consiglio in

merito al rafforzamento dello spazio cibernetico italiano, indirizzando gli attori pubblici e privati a mettere in atto i giusti provvedimenti per la sicurezza e la protezione dei sistemi nel loro complesso. Il decreto ha stabilito la divisione dei compiti degli attori politici ed amministrativi per coordinare le attività, e ha rafforzato la cooperazione fra i vari settori della vita pubblica affinché si elaborino degli efficaci meccanismi di difesa.

Dunque, molto è stato fatto, molto si sta facendo, ma ancora molto altro è da fare. Questo perché fin troppo spesso affiorano incertezze interpretative da parte della giurisprudenza in merito alle disposizioni che disciplinano il fenomeno dei crimini informatici, introdotte in Italia dalla l. n. 547/1993 e in alcuni casi modificate dopo la l.n. 48/2008. Infatti dall'analisi emerge una certa disattenzione del legislatore, che potrebbe aver agito in maniera eccessivamente superficiale per rispondere in modo rapido alla necessità di un quadro normativo, trascurando tuttavia aspetti che avrebbero permesso una maggiore chiarezza nell'interpretazione. Questa conclusione è frutto del lavoro di analisi in base alle indicazioni della dottrina, che non risulta quasi mai concorde nel dare un senso ai dettami del legislatore.

Anche a livello sovranazionale tanti passi si stanno compiendo verso una maggiore difesa dello spazio cibernetico, facendo leva soprattutto sulla necessità di cooperazione e coordinazione sia dal punto di vista investigativo che da quello giuridico. Questo aspetto è essenziale in ragione dei caratteri tipici, già evidenziati, dei crimini informatici e anche del bisogno di armonizzazione delle norme in una società quanto mai globalizzata.

Tuttavia, ci sono una serie di problemi che ancora vedono la soluzione piuttosto lontana. Due su tutti: la questione del bilanciamento fra tutela delle informazioni e

tutela della libertà personale e, connesso a questo, il problema della cd. *data retention*, della conservazione in rete dei dati che potrebbero agevolare le indagini ma che fanno parte della sfera privata degli individui. Questi ambiti sono particolarmente delicati poiché è necessario adottare comportamenti che non implichino una lesione dei diritti fondamentali ma che al contempo siano efficaci al fine della protezione dei sistemi: l'equilibrio, in questo senso, è difficile da raggiungere e ancor più difficile da mantenere.

Infine, ultimo aspetto che a mio parere va tenuto fortemente in considerazione pur non essendo strettamente giuridico, è il tema della consapevolezza in merito ai crimini informatici, al loro dilagare e alla loro centralità nella vita quotidiana. Troppo spesso, tale consapevolezza manca fra i fruitori dei sistemi informatici, poco aggiornati in merito ai rischi che si corrono lavorando con i dispositivi e navigando in rete. Tale consapevolezza è necessaria anche per una conseguente conoscenza delle destinazioni delle informazioni personali che si depositano in rete o all'interno dei sistemi informatici. Si sente fortemente la necessità di realizzare quanto i reati informatici siano quanto mai reali, oggi che le tecnologie informatiche sono parte della nostra vita e che vanno aggiornandosi continuamente. Solo partendo dal basso, con un'informazione migliorata ai soggetti che ogni giorno utilizzano e, in taluni casi, dipendono da queste tecnologie, si potrà sperare in un miglioramento della sicurezza e in una più consapevole fruizione dei vantaggi che derivano dal progresso tecnologico.