LUMSA UNIVERSITÀ | DIPARTIMENTO DI GIURISPRUDENZA (PALERMO)

Libera Università Maria SS. Assunta

Dipartimento di Giurisprudenza – Palermo

Corso di Laurea in Giurisprudenza

Cattedra di

Diritto Penale

I reati informatici: i risvolti penali dello sviluppo tecnologico

Computer crimes: the criminal implications of technological development

Relatore:

Ch.ma Prof.ssa Giorgia Cerami

Correlatore:

Ch.mo Prof. Antonino Pulvirenti

Al mio relatore, per la pazienza concessami.

A mia madre e mio padre, sempre presenti nei momenti più difficili.

A mia sorella Valeria, pronta a darmi consigli severi ma giusti.

Alla mia ragazza Anna, per avermi fatto rialzare ad ogni caduta

A me, per non essermi mai arreso, alla mia resilienza e voglia di farcela...

I REATI INFORMATICI: I RISVOLTI PENALI DELLO SVILUPPO TECNOLOGICO

SEZIONE QUARTA
(LA TUTELA DEL DOMICILIO INFORMATICO)

SEZIONE QUINTA
(LA TUTELA PREVENTIVA DEI SISTEMI INFORMATICI)
2.5 LA TUTELA ANTICIPATA IN MATERIA DI REATI INFORMATICI

SEZIONE SESTA
(LA TUTELA DELLA LIBERTÀ E RISERVATEZZA DELLA COMUNICAZIONI)
2.6 INTERCETTAZIONE IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE.

CAPITOLO TERZO
3.0 LA CONFISCA NEI REATI INFORMATICI

INTRODUZIONE

L'attuale periodo storico, la cui promessa è: apportare innovazioni alla vita umana, più velocemente di qualsiasi età precedente; ha contribuito ad un netto progresso nell'ambito sociale, culturale e lavorativo; la nascita dei moderni computer, alla portata di tutti, hanno drasticamente cambiato il modo di vivere della collettività, semplificando la vita di tutti i giorni. Oltre ogni dubbio, l'avanzamento tecnologico porta con sé l'inevitabile bisogno da parte del legislatore di creare un complesso di norme volte a fondare un sistema legislativo che assicuri la protezione di quei beni giuridici che rischiano inevitabilmente di essere compromessi tramite l'utilizzo "malevolo" di tali strumenti.

Inizialmente non era prevista alcuna tutela avverso i reati informatici, in quanto non erano considerati un pericolo per la società: a causa della scarsa conoscenza del fenomeno, tali delitti erano considerati frutto di azioni isolate e pertanto prive di rilevanza.

Nell'ultimo decennio, i mezzi informatici sono divenuti un fenomeno di massa, viene abbandonata la concezione della scarsa rilevanza di tali fatti e nasce pertanto un'attenzione peculiare verso quest'ultimi. In questo elaborato saranno analizzati, innanzitutto, proprio i progressi normativi degli ultimi anni, aventi lo scopo di reprimere le condotte criminose in materia di reati informatici.

Nel secondo capitolo saranno analizzate le fattispecie delittuose previste all'interno del codice penale, tenendo conto della normativa

vigente anche a livello sovranazionale; saranno trattati i reati elaborati in un'ottica anticipatoria della tutela penale, prendendo in considerazione le cd. norme di "sbarramento", nonché, una classificazione che tiene conto dei soggetti coinvolti e del bene giuridico leso, elementi imprescindibili al fine di delineare le numerose tipologie di reato che, ad oggi, sono previste nel novero dei comportamenti antigiuridici.

Nell'ultimo capitolo verrà effettuata un accurata analisi delle riforme introdotte con la legge 15 febbraio 2012, n.12, grazie alla quale sono state introdotte alcune nuove disposizioni in materia di confisca dei beni informatici e telematici utilizzati per la commissione di reati informatici e di destinazione dei medesimi beni, tenendo conto delle posizioni dottrinarie in tal senso.

CAPITOLO PRIMO
I REATI INFORMATICI: CLASSIFICAZIONE, EVOLUZIONE STORICA, BENI GIURIDICI

1.1 I REATI INFORMATICI: PROFILI GENERALI

Il reato informatico è un crimine tecnologico compiuto servendosi di supporti digitali, informatici o telematici, al fine di sottrarre, compromettere o distruggere beni e/o informazioni riservate.

Autorevole dottrina ha correttamente evidenziato tre aspetti principali: 1) la condotta ed i mezzi utilizzati; 2) l'oggetto materiale su cui ricade la condotta; 3) l'esistenza di particolari beni giuridici.

Per quanto attiene al primo aspetto, la condotta consiste nel danneggiare, manipolare, alterare tanto i beni che gli strumenti informatici e telematici[1].

Per quanto concerne il secondo aspetto, ossia l'oggetto materiale sul quale ricade la condotta, non si tratta soltanto di una *res* fisicamente tangibile, ma tale nozione va estesa a dati, informazioni o programmi. La peculiarità dei reati informatici ha portato la dottrina a configurare nuove figure di beni giuridici, considerati meritevoli di tutela, dotati di una loro completa autonomia rispetto a quelli preesistenti tra i quali quello dell'integrità di dati o programmi. É stato così elaborato il concetto di domicilio informatico.

É stata abbandonata la concezione originaria secondo la quale i reati informatici presupponevano particolari conoscenze tecnologiche a livello hardware e software; modello elaborato negli Stati Uniti, abbandonato a seguito di studi svolti a livello sovranazionale i quali affermano che: i Computer Crime sono figure di reato che concernono semplicemente l'informatica.

1.2 COMPUTER CRIME E CYBER CRIME: DIFFERENZE.

La diffusione della rete internet a metà degli anni Novanta, tecnologia utilizzata inizialmente soltanto a livello militare per scopi nettamente diversi da quelli utilizzati oggi dalla popolazione civile, ha contribuito, da un lato, ad una certa evoluzione sociale, culturale ed economica ma,

[1] MAURIZIO FUMO *La condotta nei reati informatici, Archivio Penale* settembre–dicembre 2013 fascicolo 3 anno LXV.

ha portato con sé anche notevoli aspetti negativi derivanti dall'uso criminoso di tali strumenti.

È emerso così un nuovo tipo di criminalità: il *cyber crime*, connesso al fenomeno di internet.

Occorre precisare che la macrocategoria dei reati informatici si suddivide in due sottoinsiemi: *cyber crime e computer crime.*

I *computer crime* contengono gli elementi tipici dei reati informatici (modalità di attuazione, oggetto su cui ricade la condotta, lesione dei particolari beni giuridici.)

Rientrano nel *Cyber crime* tutti quegli atti o fatti commessi tramite l'utilizzo della rete internet.

A titolo esemplificativo, rientrano nel *cyber crime*, gli atti di diffamazione commessi tramite l'utilizzo della rete internet, così come il reato di riciclaggio di denaro a mezzo di rete, cd. *cyberlaundering.*

Tra la cerchia dei reati informatici sono previste anche quelle figure criminose nelle quali non si porta a compimento il fatto reato, trattandosi di condotte di natura preparatoria accessoria o strumentale.[2]

1.3 L'EVOLUZIONE NORMATIVA DEI REATI INFORMATICI IN ITALIA: LE PRIME FIGURE DI REATO

La prima fattispecie riguarda "l'elaborazione dei dati", contemplata nell'art. 420 c.p. come novellato dall'art.1 dl. 21 marzo 1978 n.59, intervento in materia di terrorismo, a seguito dell'attentato al centro di

[2] L.PICOTTI*, La tutela penale della persona e nuove tecnologie dell'informazione*, Cedam, 2013 p.55

elaborazione dati della motorizzazione civile[3]. Il legislatore interviene al fine di incriminare in modo più grave il danneggiamento di impianti di pubblica utilità, di ricerca ed elaborazione dei dati, rispetto alla fattispecie di danneggiamento comune.

Tale norma diviene oggetto di revisione in seguito alla creazione di un vero e proprio complesso normativo all'interno del codice penale italiano, in materia di reati informatici, che avverrà nel 1993 con legge n. 547.

Prima, nel 1981, era disciplinato il delitto di comunicazioni o uso da parte di un pubblico ufficiale di dati ed informazioni in violazione della disciplina o dei fini previsti nella nuova normativa in tema di Pubblica Sicurezza[4].

Nel 1991, nell'ambito della legislazione speciale, si interviene per ostacolare l'uso del denaro contante con lo scopo di combattere il riciclaggio, viene inserita una figura di reato che punisce chi utilizza indebitamente carte di credito o di pagamento o altre analoghe carte che abilitino al prelievo di denaro contante o alla prestazione di beni o servizi ovvero la loro falsificazione od alterazione o il possesso, la cessione, l'acquisto di carte di tale tipo o documenti, se di provenienza illecita, o comunque falsificati o alterati.

A seguito del d.lgs. 29 dicembre 1992 n. 518, attuativo della direttiva CEE n. 91/250 del 14 maggio 1991 con riguardo alla tutela giuridica dei programmi per l'elaboratore, si ha un punto di svolta, che

[3] Si trattava, in particolare, di un attentato volto ad evitare il riconoscimento della falsità delle targhe apposte a veicoli rubati e poi utilizzati a scopi delittuosi.
[4] Art. 12 l. n.121/1981

rappresenta un intervento di natura sistematica, pur sempre nell'ambito della legislazione speciale.

Un anno dopo, a seguito delle raccomandazioni del Consiglio d'Europa, il legislatore nazionale interviene con la già citata legge n. 547, la quale apporta "modificazioni ed integrazioni alle norme del codice penale e di procedura penale in materia di criminalità informatica", una legge indispensabile al fine di contrastare gli atti criminosi commessi via computer o web, ovvero le fattispecie di danno ai sistemi informatici altrui, che la legislazione tradizionale non poteva descrivere efficacemente, se non tramite un'interpretazione in chiave evolutiva, andando però ad inficiare i principi di legalità, tassatività e determinatezza, capisaldi del diritto penale.

Gli strumenti giuridici di cui disponeva il giudice, non erano idonei a sanzionare i nuovi comportamenti *contra-legem* che iniziavano a verificarsi sul piano internazionale, nacquero così notevoli pressioni volte a ottenere una disciplina che assicurasse una risposta positiva concreta.

1.4 LA CONVENZIONE DI BUDAPEST SUL CYBERCRIME E LA SUA ATTUAZIONE

In un contesto in cui le società fanno sempre più affidamento sulle informazioni e sulla tecnologia, diventano sempre più vulnerabili al rischio della criminalità informatica.

La Convenzione sulla criminalità informatica di Budapest offre una risposta a tale rischio, non solo in Europa ma anche a livello globale:

attraverso il suo Programma sulla criminalità informatica, il Consiglio d'Europa fornisce assistenza tecnica ai paesi di tutto il mondo.[5]

Tale Convenzione, ha lo scopo di fornire un grado significativo di tutela, avverso i beni giuridici lesi dai fenomeni di *cyber-crime.*

La Convenzione prevede una serie di principi per agevolare gli Stati aderenti a conformarsi agli standard di tutela.

Viene previsto un importantissimo strumento, ovvero, un meccanismo di cooperazione tra gli organismi nazionali e internazionali.

L'accordo ha lo scopo di fornire la definizione giuridica di diverse terminologie, ad esempio la nozione di sistema informatico (da intendersi come qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico dei dati sulla base delle indicazioni fornite dal programma di software); la nozione di dati informatici (qualsiasi tipo di rappresentazione di fatti, informazioni o concetti idonei ad essere oggetto di trattamento ed elaborazione da parte di un programma o di un sistema informatico).

Il testo suggerisce agli Stati membri, un adattamento a livello normativo, di norme volte a sanzionare le condotte tipiche di aggressione ai sistemi informatici.

Gli Stati vengono invitati a punire tali fattispecie con "pene effettive, proporzionate e dissuasive, con la possibilità, di prevedere misure limitative la libertà personale[6].

[5] *Council of Europe action against Cybercrime, www.coe.int*
[6] Art. 13 della Convenzione

Nel testo della Convenzione, è prevista la responsabilità a carico delle persone giuridiche, nel caso in cui le persone fisiche abbiano commesso i delitti informatici con l'intento di soddisfare un interesse o raggiungere un vantaggio dell'ente collettivo, al quale sono legati da un rapporto di appartenenza o dipendenza.

Inoltre, le disposizioni procedurali in tema di indagini e giurisdizione, contenute nell'articolo 22 della Convenzione, si occupano di stabilire le modalità di attribuzione della competenza e della giurisdizione ad uno Stato, in caso di delitto informatico.

Sul piano nazionale, il cammino che porterà alla legge di ratifica n. 58/2008 non risulta tortuoso o complesso.

Il disegno di legge, presentato nel 2007, viene trasmesso alla Camera il 19 febbraio 2008, con il consenso "sostanzialmente" unanime, con un solo emendamento; il 20 febbraio viene approvato e trasmesso al senato; il voto finale è del 27 febbraio 2008.

Il procedimento di approvazione è effettivamente rapido, ma, porta con sé notevoli lacune ed incongruenze nella novella del legislatore, che ha voluto adeguare l'ordinamento italiano alle disposizioni del consiglio d'Europa nel più breve tempo possibile.

In sintesi, le modifiche apportate dalla 58/2008 possono essere ricomprese in una serie di sotto-gruppi: modifiche in materia di falsità informatiche (dall'intervento definitorio di documento informatico alla nuova fattispecie di false dichiarazioni al certificatore e alla nuova configurazione del delitto di frode informatica), novelle concernenti i delitti contro la sicurezza e l'integrità di dati e sistemi (la riformulazione dell'art 615 quinquies, le modifiche al reato di danneggiamento di dati

informatici, la nuova figura del danneggiamento di sistemi informatici e telematici, l'abrogazione del delitto di attentato informatico e l'inserimento delle fattispecie di danneggiamento di dati di pubblica utilità e danneggiamento di sistemi di pubblica utilità), la responsabilità da reato degli enti per i reati informatici.

1.5 REATI INFORMATICI E BENI GIURIDICI: VISIONE UNITARIA O PLURALISTICA?

Ancora oggi, il nostro ordinamento risulta privo di un sistema organico che disciplini il microcosmo dei reati informatici.
Non sono mancati in dottrina tentativi volti ad individuare un unico bene giuridico tutelato attuando una sorta di *reductio ad unum*.
Secondo alcuni autori sarebbe percepibile una dimensione unitaria del fenomeno come prodotto della tecnologia informatica telematica cibernetica; ciò al fine di individuare un unico oggetto di tutela che consista nell'affidabilità e sicurezza del ricorso alla tecnologia informatica telematica e cibernetica.
Il legislatore disciplina la materia sia nel codice penale che nella legislazione speciale.
Risulta evidente che i reati informatici siano stati collocati all'interno di titoli e capi preesistenti ovvero già preposti alla tutela di determinati beni giuridici.
Occorre individuare quali possano essere i beni giuridici della persona meritevoli di tutela nell'ambito dei reati informatici. Picotti effettua una suddivisione in quattro macrocategorie sulla base dei beni protetti. Il

primo fa riferimento ad una dimensione esclusiva e sicura di riservatezza informatica. Viene affermato come, tentando un approccio diverso da quello meramente analogico che tende ad assimilare sul piano concettuale questi "nuovi beni giuridico-informatici" con quelli tradizionalmente intesi, debba essere riconosciuto un carattere autonomo ed innovativo del predetto bene in questione. «La riservatezza informatica può essere compromessa da comportamenti potenzialmente dannosi nei confronti del sistema e dei dati, ovvero superando le misure di sicurezza ad esso relative, oppure, tramite l'accesso abusivo effettuato da soggetti privi di legittimazione, senza che sia richiesta la conoscenza di particolari e specifiche conoscenze di carattere informatico. La qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso ed alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza (chiavi fisiche o elettroniche, password, ecc.) apprestate dal titolare dello "i*us excludendi*", al fine di selezionare gli ammessi al sistema ed impedire accessi indiscriminati Il reato è integrato dall'accesso non autorizzato nel sistema informatico, ciò che di per sé mette a rischio la riservatezza del domicilio informatico, indipendentemente dallo scopo che si propone l'autore dell'accesso abusivo[7]» il mezzo di tutela consiste nel garantire la riservatezza e l'esclusività dell'accesso. Oltre all'accesso abusivo, vi sono ulteriori norme volte a tutelare il bene giuridico appena menzionato: l'articolo 615 *quater* punisce la

[7] Cass. pen. 2009, 7-8, 2828, *ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO - Configurabilità del reato - Irrilevanza dello scopo dell'accesso.*

detenzione la diffusione abusiva di codici di accesso, L'articolo 635 *bis* punisce la diffusione di dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico.

Per Quanto attiene al bene giuridico della riservatezza informatica, risulta di particolare importanza la decisione quadro dell'unione europea 205/222/GAI in il riferimento agli attacchi ai sistemi di informatici[8], allo scopo di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione la legge, tenta il riavvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi informatici. La protezione di tale bene giuridico inoltre può trovare fondamento nell'articolo 7 della carta di Nizza, la quale prevede il rispetto della vita privata.

Un ulteriore bene giuridico meritevole di tutela è la riservatezza e sicurezza delle comunicazioni informatiche.

[8] Articolo 2: Accesso illecito a sistemi di informazione 1. Ciascuno Stato membro adotta le misure necessarie affinché l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito come reato, almeno per i casi gravi. 2. Ciascuno Stato membro può decidere che i comportamenti di cui al paragrafo 1 siano punibili solo quando il reato è commesso violando una misura di sicurezza.
Articolo 3: Interferenza illecita per quanto riguarda i sistemi. Ciascuno Stato membro adotta le misure necessarie affinché l'atto intenzionale di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili sia punito come reato se commesso senza diritto, almeno per i casi gravi.
Articolo 4: Interferenza illecita per quanto riguarda i dati. Ciascuno Stato membro adotta le misure necessarie affinché l'atto intenzionale di cancellare, danneggiare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione sia punito come reato se commesso senza diritto, almeno per i casi gravi.

L’interesse del singolo si concretizza nell’interesse alla *privacy,* ovvero, nell’assenza di qualsiasi forma di accesso abusivo alle proprie comunicazioni telematiche.

Tale interesse rappresenta la declinazione più importante della libertà di espressione dei singoli.

Con riferimento alla Convenzione sul Cyber crime, è previsto l’obbligo da parte degli Stati aderenti, di punire le “intercettazioni illecite.

Nel nostro ordinamento è sempre stata manifestata particolare attenzione alla tutela di tale bene; infatti, con l’intervento legislativo del 1993 sono state previste tre fattispecie che riguardano le intercettazioni di comunicazioni informatiche e telematiche, prevedendo anche le condotte di carattere prodromico, aventi le caratteristiche di un “delitto ostacolo” (un’apparecchiatura con lo scopo di intercettare) o successive (la condotta di manipolazione di contenuti intercettati anche in maniera occasionale).

Di notevole importanza risulta inoltre il bene della protezione dei dati personali, di guisa che il legislatore è obbligato ad effettuare un bilanciamento di interessi tra la protezione della privacy del soggetto e le esigenze di trattamento dei dati, indispensabili allo svolgimento di determinate attività.

Il nostro ordinamento interno contiene norme in tema di violazioni, disciplinando le modalità essenziali per il trattamento lecito dei dati personali inserito nel Codice della Privacy, profondamente modificato ed integrato dal decreto legislativo n. 101 del 2018, che detta disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e

del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (c.d. GDPR).

1.6 COLLOCAZIONE SISTEMATICA

L'evoluzione tecnologica segue un ritmo decisamente rapido ed incalzante, ciò pone al legislatore dei problemi relativi di adeguare il complesso di norme alle costanti novità che si susseguono.
Il legislatore ha avuto cura di inserire nel testo codicistico, e non nella legislazione speciale, il nucleo fondamentale dei reati informatici. Una scelta alquanto ponderata, quella di non utilizzare una legge "speciale" per i reati informatici, ma di inserirli accanto alle norme "tradizionali" corrispondenti.
Seguendo la partizione voluta dal legislatore del 1993, è possibile distinguere i delitti introdotti nel libro II del codice penale in delitti contro la persona, inseriti nel titolo XII e delitti contro il patrimonio, contenuti nel titolo XIII.

1.7 REATI INFORMATICI: OGGETTO E CONDOTTA MATERIALE

Non è semplice individuare un bene giuridico per tutti i reati informatici. Seppur in trattazione ridotta, è possibile, però, sintetizzare degli elementi comuni per quanto riguarda l'oggetto materiale.
Fondamentale risulta la definizione di sistema informatico, contenuta nella Convenzione di Budapest: "qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati".
Si può verificare l'ipotesi nella quale siano presenti più "elaboratori", che, connessi tra loro, danno origine ad un unico "macro sistema di calcolo".
Il diritto penale prevede un solo sistema informatico, così le condotte illecite eventualmente tenute nei confronti di diversi computer saranno prese in esame in maniera unitaria. Per quanto riguarda la condotta, il soggetto attivo del reato è colui il quale impartisce ordini all'elaboratore al fine di effettuare una sequenza di operazioni.
Il dato importante è dato dalla distanza sotto il profilo temporale e spaziale, tra l'azione condotta dal reo e il risultato conseguente agli ordini impartiti al computer. Gli effetti si ripercuotono su un contesto spazio temporale diverso rispetto a quello in qui si trova il soggetto agente che ha posto in essere l'azione criminosa. Possono verificarsi fattispecie nelle quali siano coinvolti una pluralità di personal computer

(sistemi interconnessi), quest'ultimi andranno considerati in un'ottica unitaria, come un'unica violazione criminosa[9].

Tutto ciò si ripercuote sulla tematica della giurisdizione, poiché rileva ai fini dell'individuazione dell'autorità giudiziaria competente territorialmente.

Troverà applicazione la legge italiana, ai sensi dell'art 6 c.p., nel caso di scambio di dati tra sistemi operanti in Italia, ovvero, quando venga ad essere integrata in Italia solo parte della condotta o dell'evento[10]

Capitolo secondo
I REATI INFORMATICI: DISCIPLINA CODICISTICA
Sezione prima
(Reati contro il patrimonio mediante frode)

2.1.1 LA FRODE INFORMATICA: PROFILI GENERALI, DIFFERENZE CON IL REATO DI TRUFFA

L'articolo 640 ter c.p. introdotto dalla l. 23 dicembre 1993 n.547 punisce la condotta criminosa di chi "*alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*".

[9] C.SANTORIELLO E AA.VV., *I reati informatici*, p.14
[10] C.SANTORIELLO E AA.VV., *op.cit*.

Il reato di frode informatica presenta notevoli affinità con il reato di truffa ex art. 640, poiché possiede i medesimi elementi costitutivi; tuttavia, diverge da quest'ultimo per l'oggetto materiale sul quale ricade la condotta del reo atteso che non riguarda una persona (indotta in errore) bensì un sistema informatico o telematico.

Per quanto riguarda, poi, il bene giuridico tutelato vi sono due orientamenti. Secondo un primo orientamento, il reato ex art 640 ter è un reato plurioffensivo: l'azione posta in essere dal soggetto agente incide sul corretto funzionamento del sistema poiché ne altera l'assetto di fabbrica o le impostazioni predisposte dal proprietario dello stesso;

l'altro orientamento, invece, sostiene che trattasi di un reato monoffensivo, poiché la "macchina ", non può subire un pregiudizio personale dalla condotta di alterazione del sistema, così divergendo dal reato di cui all'art.640 che è, invece, un reato plurioffensivo poiché aggredisce la sfera patrimoniale ed incide sulla libera capacità di auto determinazione della vittima.

2.1.2 TRUFFA E FRODE INFORMATICA: ELEMENTI STRUTTURALI

Il reato di frode informatica, come sopra detto, presenta talune differenze con il reato di truffa; uno degli aspetti più significativi è ravvisabile nella fattispecie della condotta.

Il reato di truffa, difatti, per potersi dire integrato richiede la compresenza di due elementi: gli artifizi e i raggiri.

Per *artifizio* s'intende la simulazione o dissimulazione della realtà atta ad indurre in errore una persona per effetto della percezione di una falsa apparenza. In altri termini, è artifizio ogni comportamento idoneo a far apparire ciò che non esiste, o a nascondere ciò che esiste, e che agisca sulla realtà esterna[11].

Per *raggiro* si intende ogni attività simulatrice sostenuta da parole o argomentazioni atte a far scambiare il falso col vero[12].

Tali elementi non risultano comunque idonei al perfezionamento del reato ex art. 640 c.p, essendo richiesto un quid pluris ossia che la condotta sia idonea ad indurre in errore la vittima.

Nella truffa, pertanto, deve essere ingenerata nel soggetto passivo una visione distorta della realtà tale da farla cadere in errore.

Se, dunque, una persona può essere indotta in errore ed avere una percezione distorta della realtà, lo stesso non può dirsi per una "macchina" che esegue le operazioni per le quali è stata programmata.

Pertanto, nella frode informatica è possibile solo alterare il funzionamento della macchina senza, tuttavia, quel "quid pluris" rappresentato dalla induzione in errore.

Analizzati gli elementi costitutivi del reato di truffa ex art. 640 cp, occorre soffermarsi sulle condotte di frode informatica: 1) alterazione del processo operativo di sistema a causa delle quali lo stesso si trova a compiere operazioni non programmate; 2) intervento senza diritto , in presenza del quale, non è richiesto provocare un'alterazione del sistema

---

[11] ANTOLISEI, *diritto penale, parte speciale*, vol. I, Milano, 2002, parla di "trasfigurazione del vero". Sul punto, V. ANGELOTTI, *Delitti contro il patrimonio*, *Trattato del Florian*, 1936, 391, 414; DE MARSICO*, Delitti contro il patrimonio,* 1951; MANZINI, *Trattato di diritto penale italiano,* Vol. V, Torino, 1952.

[12] ANTOLISEI, *cit*., I, 35

anzi risulta conveniente che il sistema oggetto dell'attacco informatico funzioni correttamente (esempio di tale tipologia di attacco è rappresentato dal "Backdoor", con il quale il reo, ottiene il pieno controllo del computer della vittima da remoto, potendo in tal modo effettuare qualsiasi voglia operazione in "*input*" ed "*output*", al fine di sottrarre credenziali, informazioni, dati.)[13]

2.1.3 DISPOSIZIONE PATRIMONIALE NELLA FRODE INFORMATICA

Come abbiamo precedentemente chiarito, nella truffa l'atto di disposizione patrimoniale viene posto in essere dalla vittima; nella frode informatica invece, l'atto di disposizione patrimoniale è effettuato integralmente dal soggetto agente che, sfruttando le vulnerabilità dell'elaboratore, raggiunge il proprio intento criminoso.

La Corte di Cassazione si è pronunciata al riguardo affermando che "*il reato di frode informatica si distinguerebbe da quello di truffa, perché l'attività fraudolenta dell'agente investirebbe non una persona, quale soggetto passivo della stessa, di cui difetta l'induzione in errore, ma il sistema informatico di pertinenza della medesima, attraverso la manipolazione di tale sistema [...]*[14]*" e ancora "l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), bensì il sistema*

[13]Esempio: ottenere l'accesso al computer della vittima, in modo tale da controllarne il browser, al fine da effettuare acquisti nei siti nei quali il computer della vittima contiene le credenziali di pagamento e di accesso salvate.

[14]Cass.Pen. Sez. I, sent. 6 maggio 2011, n.17748

informatico (significativaè la mancanza del requisito della "induzione in errore") che gli pertiene è [...].[15] ”

2.1.4 CONCEZIONE DI DANNO; FRODE INFORMATICA E DOLO

Il reato di truffa prevede il ricorrere di due elementi: l'ingiusto profitto e l'altrui danno.

L’ingiusto profitto è da intendersi come qualsiasi utilità, non necessariamente patrimoniale.

Per la definizione di *“altrui danno”*, invece, si contrappongono due diverse concezioni: quella giuridica e quella economico-patrimoniale.

La prima definisce il patrimonio come “*insieme di beni economicamente valutabili facenti capo ad un soggetto”*.

Di conseguenza il “danno” si concretizza nella depauperazione patrimoniale effettiva mantenendo, nel reato di truffa, la struttura originaria voluta dal legislatore: quella di un reato di danno.

???Nel caso della frode informatica, la giurisprudenza intende qualsiasi situazione di natura sfavorevole all'insieme dei rapporti giuridici riferibili ad un soggetto, non essendo obbligatoria la *deminutio patrimonii* effettiva, avvicinando la frode informatica, a differenza della truffa nell’annovero dei reati di pericolo.

Per quanto concerne l'elemento soggettivo, è richiesto il dolo generico.

[15] Cass. Pen. Sez. VI, sent. 4 ottobre 1999, n. 3065

Tuttavia, in talune, ipotesi, è configurabile anche il dolo eventuale: fattispecie prevedute dall'agente nelle quali l'evento non è direttamente voluto dal reo ma è comunque previsto come una conseguenza possibile della propria condotta.

2.1.5 AGGRAVANTI

La frode informatica è procedibile a querela della persona offesa, ovvero dal titolare del sistema informatico o telematico; diventa un reato procedibile d'ufficio qualora ricorra una delle circostanze aggravanti, indicate dal secondo comma dell'art. 640, ovvero:
1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea 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.
3) l'avere profittato di circostanze di tempo, di luogo o di persona, anche in riferimento all'età, tali da ostacolare la pubblica o privata difesa.
4) l'avere, nei delitti contro il patrimonio, o che comunque offendono il patrimonio, ovvero nei delitti determinati da motivi di lucro, cagionato alla persona offesa dal reato un danno patrimoniale di rilevante gravità.
È da sottolineare la previsione di un aggravante speciale nel caso in cui il delitto informatico sia posto in essere dall'operatore di sistema; tale circostanza è dotata di un maggior disvalore penale in quanto tiene

conto della facilità della commissione del reato da parte di un soggetto avente tale qualifica.

Al fine di individuare la figura di colui il quale può essere considerato "system operator" è opportuno riportare la pronuncia della suprema Corte di Cassazione, la quale afferma: «*In tema di frode informatica, l'installatore di "slot machine" che provveda all'inserimento di schede informatiche dallo stesso predisposte, e tali da alterare il sistema informatico così da eludere il pagamento delle imposte previste con conseguente ingiusto profitto, assume la qualifica di operatore di sistema, rilevante ai fini dell'integrazione della circostanza aggravante prevista dall'art. 640-ter, secondo comma, cod. pen.*[16]».

2.1.6 FRODE INFORMATICA: DIFFERENZE CON ALTRI REATI

Appare opportuno, poi, evidenziare che laddove la persona offesa venga ingannata dall'agente, tramite l'ausilio di strumenti informatici e/o telematici, ovvero quando l'atto di disposizione patrimoniale venga posto in essere via telematica, è configurabile il reato di truffa e non già quello di frode informatica.

Infatti, ai fini dell'applicabilità dell'art 640 ter è fondamentale l'alterazione o l'intervento senza diritto sul sistema informatico.

Spesso tale reato viene realizzato insieme ad altre fattispecie che si

[16]Cassazione penale, Sez. II, sentenza n. 17318 del 19 aprile 2019

collocano in un contesto preparatorio alla frode informatica, quali l'accesso abusivo ai sistemi informatici (615 ter c.p.), la detenzione o diffusione di codici di accesso (615 quater c.p.), la diffusione di dispostivi o programmi volti a danneggiare o interrompere sistemi informatici (615 quinquies c.p.), i vari danneggiamenti informatici (635 bis e segg c.p.).
Malgrado ciò, risulta ammissibile il concorso con il reato di accesso abusivo dal momento che sussistono differenze in merito ai beni giuridici tutelati e alle condotte incriminate, poiché il reato di accesso abusivo tutela il domicilio informatico; invece, la frode informatica comporta l'alterazione dei dati di un sistema al fine di trarre un ingiusto profitto.

2.1.7 UN ESEMPIO DI FRODE INFORMATICA: IL PHISHING

Tra i reati che più frequentemente vengono compiuti e che ricadono, tra gli altri, all'interno della "frode informatica", vi sono le **cd. pratiche di *Phishing*.**
Trattasi, in generale, di una particolare tipologia di frode informatica realizzata sulla rete Internet attraverso l'inganno degli utenti.
Si concretizza principalmente attraverso l'invio di messaggi di posta elettronica ingannevoli, come ad esempio una e-mail, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso, previa registrazione (web-mail, e-commerce ecc.).
Il messaggio invita, riportando problemi di registrazione o di altra

natura, a fornire i propri riservati dati di accesso al servizio.
Solitamente nel messaggio, per rassicurare falsamente l'utente, è indicato un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati.
In realtà, il sito a cui ci si collega è artificiosamente allestito in modo identico a quello originale e, qualora l'utente inserisca i propri dati riservati, questi saranno nella immediata disponibilità dei criminali.
Aventi la stessa finalità, ossia carpire i dati di accesso a servizi finanziari online o altri che richiedono una registrazione, sono i virus informatici che rappresentano un pericolo ancora più subdolo dato che le modalità di infezione sono diverse; la più diffusa consiste sempre nel classico allegato al messaggio di posta elettronica. Oltre i file con estensione *.exe*, i virus si diffondono celati da false fatture, contravvenzioni, avvisi di consegna pacchi, che giungono in formato *.doc .pdf*.
Nel caso si tratti di un c.d. "*financial malware*" o di un "*trojan banking*", il virus si attiverà per carpire dati finanziari.
Altri tipi di virus si attivano allorquando sulla tastiera vengono inseriti "*userid* e *password*", c.d. "*keylogging*"; in questo caso i criminali sono in possesso delle chiavi di accesso agli account di posta elettronica o di *e-commerce*[17].
In tal caso, gli *hacker* provvedono a sottrarre la provvista dal conto e si apre una seconda fase dell'operazione criminosa avente lo scopo di far perdere le proprie tracce e, al contempo, preservare il denaro.

[17]Polizia postale e delle comunicazioni, *Phishing che cos'è? www.commissariatodips.it*

Entra dunque in gioco anche la figura del c.d. *financial manager* ovvero colui il quale accredita le somme prelevate dai *phishers* sul proprio conto corrente per poi trasferirle, in via definitiva, all'estero.
Sia la giurisprudenza che la dottrina ritiene idoneo, in mancanza di una fattispecie ad hoc, la sussunzione della fattispecie sotto il reato di truffa informatica di cui all'art. 640 ter.
La Suprema Corte ha affermato che il phishing integra la condotta di intervento abusivo (ovvero senza diritto) su un sistema informatico poiché " *l'abusivo utilizzo di codici informatici di terzi ("intervento senza diritto") – comunque ottenuti e dei quali si è entrati in possesso all'insaputa o contro la volontà del legittimo possessore ("con qualsiasi modalità") - è idoneo ad integrare la fattispecie di cui all'art. 640 ter c.p. ove quei codici siano utilizzati per intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, al fine di procurare a sé o ad altri un ingiusto profitto*".
È stata inoltre ammessa la possibile configurabilità del concorso dei delitti di frode informatica e accesso abusivo ad un sistema informatico o telematico.
Vi è un orientamento dottrinario[18] il quale prevede che la condotta del phishing consentirebbe di realizzare il concorso tra frode informatica e truffa; la ratio di tale assunto sarebbe desumibile dal fatto che il soggetto agente porrebbe in essere una condotta che consiste negli "artifizi e raggiri", inducendo in errore la vittima, tipica dell'art. 640 c.p. ed inoltre, vi sarebbe l'intervento senza diritto nel sistema informatico

[18] *Il phishing come reato informatico, la frode informatica, www.antiphishing.it*

della banca o delle poste (una volta inserite le credenziali ottenute in maniera abusiva).

Tramite queste condotte, il reo conseguirebbe proprio quell'ingiusto profitto e quell'altrui danno che sono elementi peculiari di entrambe le fattispecie.

Un elemento che merita un attenta analisi, riguarda la responsabilità penale del *financial manager.*

Ci si chiede, se siano applicabili nei suoi confronti, i reati di cui all'art.648 e 648 bis.

Il phisher, una volta portato a compimento il proprio atto criminoso deve ripulire le proprie tracce e l'ostacolo principale è rappresentato dalla movimentazione delle somme sottratte. Solitamente il phisher utilizza una serie di trasferimenti bancari nei conti dei *financial manager*, i quali successivamente "dividono" la somma di denaro in una serie di altri conti, con l'intento di farne perdere la tracciabilità, ovvero li trasferiscono in conti "*offshore*".

La problematica assume particolare rilievo nei casi in cui sia da escludere la sussistenza del dolo intenzionale o diretto in capo ai *financial manager.* La giurisprudenza è concorde nel ritenere la sussistenza del concorso di reati...., se colui il quale presta il consenso al trasferimento della somma di denaro nel proprio conto è consapevole dell'attività del phisher.

In caso contrario, ove la ignori ma sia consapevole dell'illecita provenienza delle somme di denaro, risponderà a titolo di ricettazione laddove limitatosi a ricevere le somme di denaro; risponderà di

riciclaggio se le abbia trasferite all'estero con modalità idonee ad ostacolare l'identificazione della loro provenienza delittuosa[19].
Qualora il financial manager si sia rappresentato l'eventualità della provenienza criminosa del denaro e, malgrado ciò, lo abbia ricevuto e trasferito secondo i dettami del phisher, risponderà in tale ipotesi di dolo eventuale, purché tale forma di dolo sia desumibile dalla presenza di "dati di fatto inequivoci" e non da semplici motivi sospetto[20].

2.1.8 FRODE DEL CERTIFICATORE: ART 640 QUINQUES

La fattispecie della frode del certificatore è stata inserita nell'art 640 quinques del c.p, a seguito della l.48/2008 attuativa della Convenzione di Budapest sul Cybercrime.
La norma prevede: «*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro.*»
La presente disposizione disciplina una autonoma figura di truffa (art. 640), punendo la condotta del soggetto preposto al servizio di certificazione telematica che, al fine di procurare a sé o ad altri un

[19]S. BATTAGLIA, *Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*, *Altalex* 18 settembre 2013
[20]Cass. SS.UU., Sent. 12433 del 26/11/2009

ingiusto profitto con altrui danno, viola gli obblighi certificativi previsti.

La condotta non descrive in realtà una vera e propria modalità fraudolenta del certificatore, ma il disvalore penale risulta insito nella violazione dolosa degli obblighi di certificazione.

A tale soggetto infatti la legge, per l'importanza della funzione, conferisce una particolare forma di fiducia, in vista della certificazione. Si tratta di delitto proprio dacché può essere commesso solo da quei soggetti che prestano servizi di certificazione elettronica.[21]

Mentre, l'elemento soggettivo necessario per la configurabilità del delitto di frode informatica del soggetto che presta servizi di certificazione di firma elettronica è il **dolo specifico**: premeditazione cosciente e volontaria di commettere il fatto descritto nella norma diretto a procurarsi un indebito vantaggio con altrui ingiusto danno.

Nel disegno di legge n. 2807 si faceva riferimento all'art 5 c.3, alla violazione di specifici obblighi indicati nell'art. 32 del codice dell'amministrazione digitale, al duplice evento del danno e del profitto e a un elemento soggettivo del dolo generico.

In conseguenza di un emendamento presentato e accolto dalle Camere, è nato il testo attualmente vigente il quale presenta significative differenze con quanto originariamente previsto.

A differenza di quanti previsto nel d.d.l., nel testo riferibile alla frode del certificatore viene fatto riferimento alla “violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato”,

[21] *Frode informatica nelle firme digitali, www.studiocataldi.it*

scomparendo qualsiasi accenno specifico all'art. 32 del Codice dell'amministrazione digitale.

2.1.9 LA CONDOTTA DEL CERTIFICATORE

Per quanto attiene alla condotta tipica, l'art 640 quinques contempla la violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato ossia il rilascio di un certificato [22] illegittimo ovvero in assenza dei presupposti previsti dalla legge.
La norma in esame trova la sua *ratio* nel principio del legittimo affidamento dei terzi, che quest'ultimi fanno proprio sull'operato di tale soggetto.
Oltre alla responsabilità penale prevista nei confronti del certificatore occorre menzionare l'art. 495-bis c.p. "Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri" che rappresenta un completamento proprio della fattispecie ex art. 640 ter.
La norma in esame mira a sanzionare non il certificatore, bensì coloro i quali chiedano il rilascio del certificato sulla base di false dichiarazioni o attestazioni false sull'identità, lo stato o altre qualità personali; tale condotta viene sanzionata per far in modo tale che nel certificato sia rappresentata la situazione reale di guisa da tutelare l'affidamento di coloro che si trovano in presenza di un documento sottoscritto con firma digitale.

[22] M. GROTTO, *La frode del certificatore informatico*., p.149

2.1.10 LA FORMA DI DOLO PENALMENTE RILEVANTE

L'art. 640 quinquies, come detto, sanziona il soggetto che prestando il servizio di certificazione elettronica viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Procedendo all'analisi della forma di dolo richiesta, la norma di cui all'art 640 quinques sanziona il certificatore che: "*al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno".*

Dal disposto normativo, la dottrina trae la necessaria presenza del dolo specifico nella commissione del fatto-reato con lo scopo, ulteriore, di limitare l'ambito applicativo di una determinata fattispecie; in particolare si opera come un secondo perimetro (dopo quello rappresentato dal fatto tipico) entro il quale definire la portata di applicazione.

La norma richiede che il dolo specifico vada a sorreggere la condotta oggettiva, affinché sia integrato il reato di frode del certificatore.

Il reo deve porre in essere la condotta con il precipuo fine di procurare a sé stesso o ad altri un ingiusto profitto o di arrecare altrui danno.

Il dolo specifico svolge il ruolo di delimitare il perimetro del penalmente rilevante, includendo nell'ambito applicativo della fattispecie solo le condotte idonee a raggiungere il fine prefissato.

E', quindi, richiesta non solo la rappresentazione e la volizione da parte del soggetto agente, ma anche l'efficacia causale sull'azione esterna[23].

[23] M. GROTTO, *op.cit*. p.155

2.1.11 I PROFILI DISTINTIVI DEI REATI DI FRODE INFORMATICA E INDEBITO UTILIZZO E FALSIFICAZIONE DI CARTE DI CREDITO E DI PAGAMENTO

L'Indebito utilizzo e falsificazione di carte di credito e di pagamento inserito nell'art. 493-ter c.p. dal D.lgs. 21/2018, è stato oggetto di un lungo e laborioso dibattito giurisprudenziale, al fine di chiarire se quest'ultimo, in base alle modalità di esercizio della condotta criminosa, possa essere in qualche modo ricondotto nell'alveo dei reati di cui all'art 640 ter.

La fattispecie in esame, prevista nell'attuale Codice Penale recita: «*Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.*»

Risulta fondamentale, in tale contesto, citare la pronuncia della Suprema Corte, la quale afferma: «*integra il reato di cui all'art. 55 D. Lgs. n. 231/2007 (oggi inserito nel codice penale all'art. 493 ter) la condotta di chi, senza realizzare frodi informatiche, ottenga i dati*

relativi ad una carta di debito o di credito altrui, unitamente alla stessa tessera elettronica, per poi utilizzarli indebitamente al fine di effettuare prelievi di denaro».[24]

Pertanto, è chiaro l'orientamento della Corte di inquadrare la fattispecie delittuosa nell'alveo dell'art. 493 ter, e non già dell'art. 640 ter., ogniqualvolta la condotta criminosa posta in essere dal soggetto agente non preveda la commissione di qualsiasi attività di alterazione o accesso senza diritto ad un sistema informatico.

La Corte, però, nella medesima pronuncia, afferma: «*in base a un recente orientamento della giurisprudenza di legittimità, sussiste il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, qualora il reo si serva di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, per penetrare abusivamente nel sistema informatico bancario e trasferire illecitamente i fondi ivi presenti.*»

L'utilizzazione fraudolenta del sistema informatico rappresenta, dunque, l'elemento specializzante rispetto alla generica indebita utilizzazione dei codici d'accesso di cui all'art. 493 ter c.p.

Sicché, sussiste il reato di cui all'art. 640 ter c.p. anche qualora il reo, entrato in possesso dei codici senza ricorrere a raggiri, all'insaputa o contro la volontà del legittimo titolare, intervenga su informazioni e dati contenuti in un sistema informatico o telematico al fine di procurare a sé o altri un ingiusto profitto.

[24]Corte di Cassazione, sez. II penale, sentenza 12 dicembre (ud. 30 ottobre 2019), n. 50395/2019

Sulla base di quanto affermato, sono diverse le finalità protettive delle due norme incriminatrici; il reato di cui all'art 493 ter c.p. tutela non solo il patrimonio individuale, ma anche l'interesse generale al regolare svolgimento dell'attività finanziaria attraverso mezzi sostitutivi del contante.

Si può dunque far riferimento alle generali categorie dell'ordine pubblico economico e della fede pubblica.

L'art. 640 ter c.p., dal canto suo, è collocato tra i delitti contro il patrimonio, esso mira a tutelare il patrimonio da comportamenti fraudolenti, il regolare funzionamento di sistemi informatici e la riservatezza dei dati ivi contenuti.[25]

[25] ENRICA OBERTO*, I profili distintivi dei reati di frode informatica e di indebita utilizzazione delle carte di pagamento, www.iusinitinere.it*

SEZIONE SECONDA

(reati contro la fede pubblica)

2.2 IL REATO DI FALSO INFORMATICO

2.2.1 IL FALSO INFORMATICO: EVOLUZIONE GIURIDICA

L'art 491 bis c.p., avente ad oggetto il reato di falso informatico, trova la sua ratio nel crescente bisogno di estendere la disciplina della falsità anche ai documenti informatici, tutelando il bene giuridico della fede pubblica da intendersi come affidamento della collettività sulla genuinità di determinati documenti e nei fatti in essi rappresentati.[26]

Tale fattispecie è stato introdotta dalla legge n. 547 del 23 dicembre 1993 e poi modificata dall'art. 3 della legge di ratifica della Convenzione del Consiglio d'Europa sul Cyber crime del 18 marzo 2008; successivamente, è stata oggetto di un ulteriore revisione per opera del d.lgs. 15 gennaio 2016, n. 7, in conseguenza della quale qualsiasi estensione della disciplina penale sulla falsità degli atti ai documenti informatici privati deve ritenersi esclusa (a tali documenti si applicheranno le sanzioni civili previste dal D.L.vo n.7/2016 per i falsi nelle scritture private[27]).

In particolare, come per gli atti, le condotte di reato potranno configurarsi come "falsità ideologica" (quando nell'atto – documento

[26]C.SANTORIELLO E AA.VV., *I reati informatici,* pag.28

[27]*Falso Informatico, avvocatopenletorino.it*

sono contenute attestazioni o dichiarazioni non veritiere) o come "falsità materiale" (quando esiste una divergenza tra autore apparente ed autore reale del documento o quando il documento sia stato alterato dopo la sua formazione).

Tanto premesso, per una definizione di documento informatico deve farsi ora riferimento al Codice dell'Amministrazione Digitale - D.lgs. 7 marzo 2005 n. 82, che nel suo articolo 1, lett. P, afferma essere tale "l*a rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

Infatti, la precedente definizione contenuta nell'art. 491 bis, come originariamente formulato, è stata soppressa dalla citata legge 48/2008. Con la novella, si è anche eliminato il riferimento ai programmi, i quali trovano adesso o tutela nelle norme relative al danneggiamento informatico (artt. 635 bis e 635 ter c.p.) in caso di loro manomissione illegittima.[28]

Al fine di stabilire il concetto di documento informatico occorre far riferimento alle assai numerose norme in materia di documenti informatici che nel corso di questi anni sono state emanate, nonché alle valutazioni della dottrina e della giurisprudenza.

Una volta chiarito in quali casi ci troviamo di fronte ad un documento informatico pubblico, la concreta tutela penale dovrà ricavarsi dall'applicazione di uno dei delitti in tema di falso in atto pubblico previsti dal Capo II del Titolo VII del Libro II del codice Penale.

[28] *MAXIME MANZAR*I, *I reati informatici in particolare: il falso informatico, maximemanzari.com*

Ai fini dell'applicazione delle norme sul falso informatico la giurisprudenza ha ritenuto di applicare l'art.491 bis c.p., unitamente alle norme che descrivono di volta in volta la fattispecie tipica, nei seguenti casi:

- notaio che attesta falsamente in documenti informatici relativi all'autoliquidazione delle imposte fatti dei quali gli atti erano destinati a provare la verità (artt.480-491 bis c.p.);
- inserimento di dati relativi al superamento di esami mai sostenuti su un supporto informatico, concernente il proprio curriculum universitario, che abbia funzione vicaria dell'archivio dell'Università e, pertanto, destinazione potenzialmente probatoria, quantomeno provvisoria (artt.483 – 491 bis c.p.);
- pubblico ufficiale che, in qualità di addetto al servizio di inserimento dati nel sistema di verbalizzazione informatica, alteri documenti informatici pubblici relativi alla predisposizione di verbali di accertamento di violazioni di norme del codice della strada (artt.476 – 491 bis c.p.);
- confezionamento di un falso atto informatico destinato a rimanere nell'archivio informatico di una p.a. da parte di un pubblico ufficiale nell'esercizio delle sue funzioni (artt.476 e 479 – 491 bis c.p.).[29]

[29] *Falso Informatico, avvocatopenletorino.it*

2.2.2 LA NOZIONE DI ATTO PUBBLICO

Al fine di stabilire la pubblicità di un atto, non è richiesto soltanto che sia posto in essere da pubblico ufficiale o incaricato di pubblico servizio.

All'uopo la Corte ha individuato dei requisiti a tal fine.[30]

Viene precisato che: "l'*estensione del concetto di documento pubblico presenta senz'altro una ampiezza maggiore rispetto a quanto desumibile dall'art. 2699 c.c. perché devono essere ricompresi, oltre ai documenti stilati, secondo le formalità prescritte, da parte di un notaio o di un qualsiasi altro pubblico ufficiale autorizzato ad attribuirvi pubblica fede, quei documenti formati da pubblico ufficiale o dal pubblico impiegato incaricato di pubblico servizio nel corso dell'esercizio delle sue funzioni o del suo servizio, attestanti fatti da lui compiuti o avvenuti in sua presenza e aventi attitudine ad assumere rilevanza giuridica"*[31].

E 'importante, sottolineare infatti, che non tutti gli atti compiuti da questi soggetti sono, in via automatica, da considerarsi atti pubblici: "sarà sempre necessario un nesso tra l'attività falsificatrice e l'esercizio delle pubbliche funzioni o del pubblico servizio".

Proprio basandosi su questo principio, la Cassazione ha escluso l'applicabilità degli artt. 479 e 491 bis c.p. nell'ipotesi di falsificazione del badge attestante la presenza di pubblici dipendenti sul luogo di lavoro poiché riferibili a circostanze (la presenza a lavoro)

[30]Cass., s.u. 11 aprile 2006 n.15983
[31]C.SANTORIELLO E AA.VV., *op.cit*., pag. 33

inerenti alla disciplina privatistica e non dichiarazioni concernenti l'attività della pubblica amministrazione.
Secondo questa lettura interpretativa, saranno considerati atti pubblici soltanto quelli formati da un pubblico ufficiale o da un pubblico impiegato incaricato di pubblico servizio e compilati, con le prescritte formalità, per uno scopo di diritto pubblico, inerente all'esercizio della propria funzione o del pubblico servizio, al fine di comprovare un fatto giuridico o di attestare fatti da lui compiuti o avvenuti in sua presenza ed aventi rilevanza giuridica (Cass. 17-7-1990, n. 10414).

2.2.3 FALSO INFORMATICO, PUNIBILITÀ

Ai fini della punibilità dei reati di cui all'art. 491 bis c.p., l'articolo opera un rinvio alle norme in tema di falsità di atti e ciò si ripercuote anche sotto il profilo della punibilità riguardante il soggetto che fa uso del documento informatico falso, pur senza aver concorso nella condotta falsificatoria.
La dottrina è concorde nel sostenere sia la punibilità di tale soggetto quando utilizzi il documento in questione, sia nel caso in cui vi sia stato concorso nella condotta di falsificazione.
Basti pensare all'ipotesi nella quale il reato di falso venga commesso all'estero e il reo abbia fatto uso del documento falso in Italia, o al caso in cui il reato di falso sia estinto e il reo ne faccia uso: anche in tali ipotesi la responsabilità penale non verrà esclusa.

2.2.4FALSIFICAZIONE E DOLO

Malgrado la Convenzione di Budapest avesse indicato agli Stati membri di elaborare le fattispecie di falso disciplinando il momento punitivo nel caso di condotta commessa in via fraudolenta o con altro analogo intento delittuoso, il legislatore italiano ha optato semplicemente per un rinvio per relationem al complesso normativo in tema di falso in atto pubblico.

Ciò comporta che, nelle fattispecie in esame, si prevede come elemento soggettivo il solo dolo generico non essendo richiesta né l'intenzione di nuocere né la consapevolezza della produzione di un danno.

SEZIONE TERZA

(REATI CONTRO L'INTEGRITÀ DI DATI E PROGRAMMI INFORMATICI)

2.3 IL DANNEGGIAMENTO INFORMATICO

2.3.1 I DANNEGGIAMENTI INFORMATICI: EVOLUZIONE STORICA

Durante gli anni '70, la giurisprudenza si è trovata di fronte all'esigenza di inquadrare normativamente tali ipotesi; i primi tentativi consistettero nel ricondurle al quadro delle norme tradizionali, tra cui il danneggiamento di cose ex art. 635 c.p.

Tuttavia, se da un lato non sorgevano particolari problemi con riguardo ai casi di danneggiamento dell'hardware (la parte fisica di un computer), grosse perplessità sorgevano per quanto concerneva le condotte aggressive aventi ad oggetto dati e programmi.

Anche queste ultime, in un primo momento, venivano ricondotte per analogia nell'alveo dell'art. 635 c.p.[32] pur trattandosi di danneggiamento "logico" e non più fisico; veniva infatti sostenuto che la condotta causante l'alterazione dei programmi e dei dati contenuti in un sistema avesse l'effetto concreto di condurre ad una "invalidazione funzionale o strutturale della parte hardware"[33].

[32]Il danneggiamento comune viene depenalizzato dal legislatore nel 2016.

[33]I.SALVADORI*, Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, *rivista di dir. e proc. Penale,* p. 205

La definizione di sistema informatico era intesa come: “connubio indivisibile tra apparecchiature fisiche hardware e i programmi che le utilizzano e specializzano”[34].

Una siffatta impostazione però incontrava almeno due generi di limiti: da un lato la presunzione secondo la quale ogni alterazione riguardante dati e programmi informatici avesse come conseguenza il danneggiamento del relativo supporto hardware; dall'altro, non venivano presi in considerazione i casi di danneggiamento o manomissione di dati in fase di trasmissione (es. i dati passanti attraverso la rete internet).

In Italia la prima norma, destinata a sanzionare specificatamente il danneggiamento informatico, è stata introdotta dalla legge n. 547 del 1993 la quale ha inserito nell'impianto codicistico l'art. 635 bis c.p..

Il secondo grande passaggio riformatore è avvenuto grazie alla ratifica della Convenzione di Budapest, con la quale viene considerata la scelta di sanzionare, in via autonoma, il danneggiamento di sistemi informatici e telematici altrui inserendo nel complesso normativo l’ art. 635 quater c.p..

La legislazione penale, attualmente, prevede una quadripartizione in materia di danneggiamento informatico, al fine di differenziare le fattispecie incriminatrici sulla base di una maggior o minor rilevanza ai fini pubblicistici[35].

La tutela del patrimonio informatico poggia su due pilastri principali:

[34]Cfr. Pretura di Torino, 23 ottobre 1989, Vincenti e altro, Dir, in. Inf.; 1990, 620 ss.

[35]Relazione d'accompagnamento al d.d.l. n.2807, 8.

1. danneggiamento di informazioni, dati e programmi informatici, i quali trovano tutela nell'art 635 bis c.p
2. danneggiamento di sistemi informatici e telematici, tutelati dall'art 635 quater.

Qualora la condotta del soggetto agente abbia ad oggetto l'aggressione a sistemi o informazioni di pertinenza dello Stato, di altri enti pubblici o comunque di pubblica utilità, in questi casi è prevista l'applicazione di due norme diverse, ovvero l'art 635 ter c.p. e l'art 635 quinques c.p.. Importante sottolineare come tali fattispecie hanno addirittura anticipato la tutela prevedendo la sanzione anche a prescindere dal verificarsi di un effettivo danneggiamento, ritenendo sufficiente un'azione diretta a produrlo.[36]

2.3.2 L'ARTICOLO 635 BIS DEL CODICE PENALE: DANNEGGIAMENTO DI INFORMAZIONI, DATI O PROGRAMMI INFORMATICI

Sulla base di quanto evidenziato nel paragrafo precedente, il danneggiamento di informazioni, dati o programmi è disciplinato dall'art. 635 bis del c.p., il quale recita: "*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero*

[36] *Forme di danneggiamento informatico: art.635*, *avvocatopenaletorino.it*

con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".

La norma è collocata nel Libro II – Dei delitti in particolare; Titolo XIII – Dei delitti contro il patrimonio; Capo I – Dei delitti contro il patrimonio mediante violenza alle cose o alle persone. Il secondo comma è stato così sostituito dall'art. 2, 1° co., lett. m), D.Lgs. 15.1.2016, n. 7, a decorrere dal 6 febbraio 2016.

L'art. 635-bis c.p. ha ad oggetto la protezione, in via esclusiva, del software o dei dati e/o delle notizie in esso contenute (invalidazione funzionale delle componenti immateriali), ferma l'applicabilità della disposizione generale sul danneggiamento per ciò che riguarda la tutela dell'inviolabilità della parte fisica delle apparecchiature informatiche o telematiche (invalidazione materiale).

L'oggettività giuridica è costituita dall'integrità del patrimonio e da beni di natura non meramente patrimoniale, quali gli interessi all'integrità ed alla funzionalità dei dati e dei programmi informatici.

Continuando l'analisi normativa dell'art 635 bis c.p., occorre soffermarsi sull'elemento della condotta; esso consiste nella «distruzione», nel «deterioramento», nella «cancellazione», nell'«alterazione» e nella «soppressione» di informazioni, dati o programmi informatici altrui. La fattispecie, che riflette un reato di evento a forma libera, può essere integrata anche mediante un comportamento omissivo.

Quanto alla nozione di «altruità», l'art. 635-bis c.p., richiede l'«altruità» dei beni oggetto di danneggiamento informatico. Stante la difficoltà di individuare la persona offesa sulla base

dell'«altruità», in dottrina, si è proposto di fare riferimento a tutti gli interessi giuridicamente rilevanti, di natura obbligatoria, che confluiscono sui dati facendo leva sulla figura dell'«interessato» (ovverosia la persona cui i dati si riferiscono) introdotta dal Codice Privacy (D.lgs. 196/2003).

La clausola di riserva posta all'incipit della norma circoscrive l'ambito di operatività dell'art. 635-bis c.p. all'aggressione alla integrità fisica o logica di informazioni, dati o programmi non sussumibili in fattispecie astratte diverse e più gravi (es. falsità per soppressione ex art. 491-bis c.p. e accesso abusivo a sistema informatico o telematico ex art. 615-ter c.p., qualora a tale reato segua il danneggiamento).

Per "*soppressione*" deve intendersi sia le condotte che cagionano una eliminazione definitiva dei dati (impedendo qualsiasi possibile recupero) sia quelle impeditive dell'accesso da parte dell'avente diritto, anche aventi effetti solo temporanei.

Per quanto attiene alla nozione "*cancellazione di dati*", essa consiste nel rendere completamente e definitivamente irriconoscibile il contenuto di dati o programmi.

Degna di nota risulta la pronuncia della suprema Corte secondo la quale, non viene esclusa la responsabilità penale del soggetto agente, malgrado l'avente diritto riesca a ripristinare la situazione *ex-ante*: « *il reato ex art. 635-bis c.p. deve ritenersi integrato anche quando la manomissione e l'alterazione dello stato di un computer sono rimediabili soltanto attraverso un intervento recuperatorio postumo, comunque non reintegrativo, dell'originaria configurazione dell'ambiente di lavoro (in specie, la S.C., ha ritenuto la sussistenza del*

reato in un caso in cui era stato cancellato, mediante l'apposito comando e, dunque, senza determinare la definitiva rimozione dei dati, un rilevante numero di file, poi recuperati grazie all'intervento di un tecnico informatico specializzato) [37] *. »*

Con riguardo alla condotta di "*distruzione*", essa è diretta ad un mezzo fisico, mentre il "*deterioramento*" ricopre i fenomeni che hanno ad oggetto il peggioramento del "bene" inteso quale *res* tangibile e non.

Nell'annovero degli atti diretti a "deteriorare" rientrano a titolo esemplificativo quelle attività tra le quali, lo *spamming*, nel caso in cui arrivi a saturare volontariamente, con un elevato numero di comunicazioni a distanza ravvicinata, le risorse di un computer, nonché, il c.d. "attacco DDos" acronimo di: *Distributed Denial of Service*, consiste nel tempestare di richieste un sito web, con lo scopo di saturare il server e renderlo irraggiungibile per un periodo temporale più o meno lungo.[38]

Stando agli ultimi dati del Clusit, l'associazione italiana per la sicurezza informatica, è tra gli attacchi che colpiscono un'impresa ogni cinque minuti insieme ai *malware* e ai *ransomware*.[39]

Occorre rilevare come il legislatore italiano non abbia scelto di limitare la previsione penale ai casi gravi di danneggiamento di dati e programmi (una possibilità che veniva offerta dall'articolo 4 della

[37]CORTE DI CASSAZIONE, SEZ. II, 15.9.2016, N. 38331

[38]Essenzialmente un DDoS avviene mediante l'invio di pacchetti "falsificati" ad una macchina obiettivo; in caso di DDoS (distribuito su più IP), a differenza del DoS "singolo", i pacchetti sono smistati secondo una logica idonea atta ad **espandere esponenzialmente**, ad ogni livello successivo, l'effetto dell'attacco.

[39]*ROSITA RIJTANO, Attacco DDoS (Distributed Denial of Service): Cos'è, come fare, come difendersi. www.cybersecurity360.it*

Convenzione sul Cybercrime di Budapest e dall'art. 3 della Decisione Quadro 2005/222/GAI).

La previsione di una tale clausola si porrebbe lo scopo di limitare l'area applicativa del fatto tipico, escludendo i casi di danneggiamenti di dati privi di valore o di qualsivoglia utilità.

L'ineliminabile carattere elastico della c.d. "gravità" del danneggiamento pone non pochi problemi ai giudici chiamati ad individuare un parametro che in concreto discrimini i fatti gravi da quelli non gravi.

Il reato è procedibile mediante querela della persona offesa.

Riguardo al campo di applicazione delle aggravanti, antecedentemente al 2008, veniva fatto un rinvio alle aggravanti dell'art 635, co. 2, c.p.

Ciò suscitava non poche problematiche applicative in giurisprudenza e perplessità da parte della dottrina perché, escludendo le ipotesi nelle quali il fatto viene commesso avvalendosi di violenza o minaccia, tali circostanze risultavano non applicabili nel contesto di un danneggiamento informatico.

Nel contesto attuale, per quanto riguarda il rinvio alle aggravanti del danneggiamento, il secondo comma dell'art. 635bis del codice penale prevede un aggravamento di pena qualora il fatto sia commesso con violenza alla persona o minaccia, ovvero con abuso della qualità di operatore del sistema.

Con riferimento "all'abuso della qualità di operatore di sistema", essa sussiste quando l'agente abbia strumentalizzato la predetta qualità ai fini della realizzazione della condotta; l'aggravante de qua non intende riferirsi alla titolarità astratta di una particolare qualifica professionale

o tecnica nel settore informatico, ma vuole piuttosto sottolineare il momento di collegamento funzionale (anche se occasionale) di un determinato soggetto per ragioni inerenti ai suoi compiti professionali, con il sistema informatico,[40] In conseguenza della integrazione di suddette circostanze, il reato diviene procedibile d'ufficio e la pena vede un aumento nella cornice edittale.

L'elemento soggettivo del reato è il dolo generico, da intendersi quale coscienza e volontà del fatto tipico, non dovendo l'agente perseguire alcun fine specifico, ma solo avere la consapevolezza di distruggere, deteriorare, cancellare, alterare o sopprimere i beni informatici protetti.[41]

2.3.3 L'ARTICOLO 635 TER DEL CODICE PENALE: DANNEGGIAMENTO DI DATI O PROGRAMMI PUBBLICI

La fattispecie di cui all'art. 635 ter c.p. sanziona i fatti di danneggiamento descritti all'art. 635 bis c.p. quando abbiano ad oggetto "*informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità".*

La tutela penale è rivolta all'integrità di dati che assumono oltre ad un'elevata utilità, un alto interesse sociale.

[40] *Danneggiamento di sistemi informatici e telematici, www.101professionisti.it*

[41] AVV. FRANCESCO ALBANESE E AVV. VALENTINA PRIVITERA*, La criminalità informatica in Italia*, pag27,28,29

Viene criticato in dottrina il ricorso, da parte del legislatore, in quanto privo di giustificazione politico-criminale, alla scelta di ricorrere ad espressioni diverse per definire "oggetti passivi" aventi identica rilevanza pubblica in luogo della complessa e controversa locuzione *«utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità»* per qualificare gli "oggetti" su cui ricadono le modalità lesive previste dall'art. 635-ter c.p..[42]

Criticata risulta inoltre la scelta di modellare le fattispecie di danneggiamento di dati e di sistemi informatici «di pubblica utilità» su quella del delitto di attentato ad impianti di pubblica utilità, di cui all'art. 420 c.p. (parzialmente abrogato dall'art. 6 l. 48/2008), anziché — come sarebbe stato più corretto — sulle ipotesi base di danneggiamento di dati (art. 635-bis c.p.) e di sistemi informatici (art. 635-quater c.p.).

Identici, rispetto all'abrogato comma 2 dell'art. 420 c.p., sono non solo il trattamento sanzionatorio (reclusione da 1 a 4 anni nell'ipotesi base; da 3 a 8 anni nell'ipotesi aggravata), ma anche la tecnica di formulazione.

Rispetto alle ipotesi base, gli artt. 635-ter, comma 1, c.p. e 635 quinquies, comma 1, c.p., si caratterizzano per la peculiare struttura di delitti di attentato («fatti diretti a») e, di conseguenza, per l'anticipazione del momento consumativo.

La struttura dell'art. 635-ter, comma 2, c.p. è stata invece modellata su quella dell'abrogato comma 3 dell'art. 420 c.p.

[42] Sul punto cfr. le considerazioni critiche di Picotti L., *La ratifica della Convenzione Cybercrime*, cit., 715.

Si sono così introdotte in questo complesso "microsistema" normativo sui danneggiamenti informatici due fattispecie, la cui struttura («se dal fatto deriva») è apparentemente analoga a quella dei «reati aggravati dall'evento ».[43]

2.3.4 IL DANNEGGIAMENTO DI SISTEMI INFORMATICIPROBLEMI INTERPRETATIVI: 635 *QUATER* C.P. E 635 *QUINQUIES*

Gli artt. 635 quater c.p. e 635 quinquies puniscono le condotte che comportano il danneggiamento del complessivo sistema informatico e non di singoli dati e programmi.
Particolari difficoltà applicative rischiano di presentare la condotta consistente nell'ostacolare gravemente il funzionamento del sistema, in particolare considerando la configurazione come "reato di pericolo" emergente dal comma 1 dell'art. 635 quinquies c.p.
È evidente che con riguardo a tale fattispecie si sia scelto di allontanarsi dall'art. 635 ter.
Difatti, mentre quest'ultimo sanziona il fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di pubblica utilità, il primo comma dell'art. 635 quinquies prevede un reato a forma vincolata.

43
IVAN SALVADORI, il "microsistema" normativo concernente i danneggiamenti informatici. un bilancio molto poco esaltante, Riv. it. dir. e proc. pen., fasc.1, 2012, pag. 204

Viene fatto un rinvio alla norma ex 635 quater c.p.: “se il fatto di cui all'art. 635 quater è diretto a”.
In dottrina, si sostiene che in tal modo si voglia punire solo e soltanto gli atti miranti a distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici di carattere pubblico o ad ostacolarne gravemente il funzionamento, commessi secondo le modalità indicate dall'art. 635 quater c.p.
È doveroso sottolineare che non sia necessario un danno “irreparabile all’elaboratore” tale da comportare una totale incapacità di funzionamento del sistema, essendo sufficiente che si configuri un “serio ostacolo” al suo normale funzionamento[44].
Il legislatore, nella formulazione delle fattispecie di cui all'art. 635 quater c.p., ha tenuto debitamente conto della dilagante diffusione dei virus informatici tanto da prevedere anche il danneggiamento mediante introduzione o trasmissione di dati, informazioni o programmi.

SEZIONE QUARTA
(LA TUTELA DEL DOMICILIO INFORMATICO)

2.4. ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO

La norma dell'accesso abusivo ad un sistema informatico o telematico

[44] AA.VV. SANTORIELLO, *op.cit.*, p. 83

ha trovato applicazione in misura sensibilmente superiore rispetto a tutti gli altri reati informatici e ciò ha consentito un considerevole sviluppo sul piano giurisprudenziale.

Tutto questo ha comportato la nascita di diversi orientamenti sia dal punto di vista della finalità che dal punto di vista applicativo.

Secondo parte della dottrina [45], sono due le principali ragioni che hanno portato all'introduzione di questa figura di reato nel codice penale.

La prima risalente alla fine degli anni '70, era dettata dall'esigenza di una risposta sanzionatoria ai casi di spionaggio informatico (si faccia riferimento all'indebita acquisizione di dati o strumenti software, frutto di ricerche e studi da parte di un'impresa).

Le norme vigenti, con riguardo alla inviolabilità dei segreti, non risultavano adeguate allo scopo[46] e lo stesso reato di furto contenendo la dizione di "cosa mobile" non pareva poter comprendere i dati o programmi informatici.

La seconda era quella di contrastare il fenomeno, sempre più diffuso, degli "hacker"[47] : premettendo che non ne esiste una sola definizione, per il nostro studio facciamo riferimento a quei soggetti che, utilizzando un elaboratore collegato alla rete internet, riescono ad entrare in comunicazione con diversi sistemi informatici collegati ad essa e bypassare le misure di sicurezza informatiche a scopo malevolo.

---

[45] C.PECORELLA, *il diritto penale dell'informatica*, p.253 e ss.

[46] G. ARONICA, *l'indice penale 2010*, p.200.

[47] È opportuno sottolineare come parte della dottrina preferisca fare propria la distinzione tra "cracker" e hacker" definendo il primo come colui che supera le misure di sicurezza al fine di accedere al sistema senza essere autorizzato. La figura dell'hacker invece consta in un soggetto altamente preparato in campo informatico dedito allo studio dei codici di programmazione: l'accesso abusivo in sistemi altrui avrebbe solo un fine dimostrativo ma non volto al danneggiamento di dati e programmi.

Questa figura di criminale informatico, sorta negli anni '80, nella realtà contemporanea si è oramai affermata e sono sempre più numerosi i Paesi che prevedono strumenti giuridici volti a contrastare tale dilagante fenomeno.

Il legislatore italiano però è intervenuto solo a seguito di un impulso di matrice europea: la Raccomandazione n. R (89) 9 del 13 settembre 1989 che si occupava di criminalità informatica.

Al suo interno era possibile rinvenire due gruppi di infrazioni per le quali si raccomandava la previsione di figure di reato nei Paesi Membri. Accanto ad una c.d. lista minima, contenente le condotte criminose per le quali era più urgente una previsione normativa, figurava una seconda lista "facoltativa" dove era rimessa alla discrezionalità dei vari governi la scelta sul se elaborare fattispecie incriminatrici o meno.

Nella lista primaria era incluso l'accesso non autorizzato, "l'archetipo dell'attuale fattispecie di accesso abusivo".[48]

Per la sua entrata in scena nel panorama penalistico italiano si dovrà aspettare la l. n.577 del 1993 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica".

L'art 4 della l. n.547/1993 la introduce nella Sezione IV che tutela "l'inviolabilità del domicilio" del Capo III "delitti contro la libertà individuale", Titolo XII "delitti contro la persona" del libro II del codice penale).

[48]G. ARONICA, *l'indice penale 2010*, p.202

La fattispecie di cui all'art. 615-ter c.p. è stata inserita tra i delitti contro l'inviolabilità del domicilio, in quanto «i sistemi informatici o telematici (...) costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale»[49].

Il rapporto di simmetria con la violazione di domicilio, peraltro, non attiene soltanto al bene giuridico tutelato (il domicilio, rispettivamente fisico ed informatico), ma abbraccia anche la struttura della fattispecie, delineata sulla falsariga dell'art. 614 c.p.

Nel delineare questo rigido parallelismo, il legislatore italiano ha seguito la strada tracciata dalla Raccomandazione del Consiglio d'Europa del 1989 che, individua nell'inviolabilità del computer domiciliare l'interesse che l'incriminazione dell'accesso abusivo mira a tutelare ed evidenzia la diretta derivazione di tale previsione incriminatrice dalla tradizionale figura di house- breaking e, dunque, dalla tutela del domicilio fisico.

2.4.1 L'ART 615 TER DEL CODICE PENALE: PREVISIONE NORMATIVA E CARATTERI ESSENZIALI

L'accesso abusivo ad un sistema informatico o telematico è un delitto punito dall'art. 615-ter del codice penale, il quale, dispone che *"chiunque abusivamente si introduce in un sistema informatico o*

[49] Relazione di accompagnamento al d.d.l. n. 2773 del 1993, cit., p. 9.

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."

"La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva 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.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque, d'interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

L'accesso abusivo ad un sistema informatico si verifica, quindi, nella ipotesi in cui un soggetto si introduce in un sistema informatico o telematico protetto da misure di sicurezza.

La seconda ipotesi si verifica allorché un soggetto autorizzato ad

accedere ad un sistema informatico vi si trattenga successivamente al periodo temporale necessario a giustificare la presenza nello stesso sistema per il quale aveva ricevuto la autorizzazione (concetto che delineeremo più avanti riguardo una pronuncia della Suprema Corte)
In entrambi i casi si può parlare di reato di azione, in quanto il reato consiste nel semplice compimento dell'azione e, precisamente, di un reato di azione commissivo poiché la condotta tipica è rappresentata da un agire positivo.
Tale reato può essere commesso da chiunque ed è di tipo mono soggettivo, non richiedendo la partecipazione di una pluralità di soggetti agenti.
L'illecito si consuma con l'introduzione nel sistema informatico o telematico, contro la volontà del titolare, nella prima ipotesi; con la permanenza contro tale volontà nella seconda ipotesi.
In merito alla forma, il reato è sicuramente a forma vincolata perché la sua realizzazione presuppone una determinata condotta, che si realizza con l'introduzione abusiva o con il mantenimento abusivo.
Trattasi di un reato di pericolo, poiché esiste il rischio che chi accede abusivamente a un sistema abbia la capacità di impadronirsi o venire a conoscenza dei dati in esso contenuti.
In merito alla successiva suddivisione, approntata dalla dottrina, tra reati di pericolo concreto e reati di pericolo presunto, nei primi il pericolo è elemento costitutivo della fattispecie incriminatrice mentre nei secondi il pericolo si presume.
Il reato di accesso abusivo di cui all'art. 615-ter c.p. risulta essere,
Trattasi, inoltre, di un reato che richiede il dolo generico in quanto colui

che accede abusivamente o si intrattiene contro la volontà del dominus, ha in sé la coscienza e la volontà di realizzare gli eventi costitutivi di un reato.

2.4.2 CIRCOSTANZE AGGRAVANTI

Vengono previste, ai commi 2 e 3, diverse circostanze aggravanti. Tra quelle previste al comma 2, quelle ai nn. 1 e 2 corrispondono alle aggravanti dei delitti di interferenze illecite nella vita privata ex art. 615 bis.

Merita attenzione la previsione dell'aggravante dell'abuso della qualità di operatore del sistema.

Questo soggetto ha maggiori possibilità di accedere al sistema informatico, ad aree riservate e di controllarne le operazioni.

L'aggravante in questione trova la sua giustificazione proprio nella esigenza di sanzionare la posizione di colui il quale si trova in una situazione privilegiata nel compimento del reato, ovvero, per punire il tradimento della fiducia riposta dal titolare nell'operatore del sistema.

Su chi possa, sostanzialmente, esser considerato "operatore di sistema" ai fini dell'applicazione della aggravante, la dottrina sostiene diverse ipotesi.

Se alcuni ammettono la possibilità di definire tale anche il tecnico nonché qualsiasi soggetto che, per le funzioni svolte, si trova ad intervenire sul sistema[50], altri escludono categoricamente dalla nozione di "system operator" coloro che, pur abilitati ad operare nella console

[50]C.SANTORIELLO E AA.VV., *op.cit.,* pag. 67

dell'elaboratore, dispongono solo di una conoscenza limitata o settoriale del sistema che non fornisce, di conseguenza, quel maggiore vantaggio di cui gode l'operatore del sistema nella commissione del reato.

Infine, è opportuno puntualizzare come la qualità di operatore del sistema non debba necessariamente avere una certa dimensione quantitativa, essendo sufficiente anche una attribuzione occasionale.

Va anche ricordata l'aggravante prevista nel co.2 al n.3: l'ipotesi in cui dall'accesso abusivo derivi il danneggiamento del sistema nel suo complesso o di singole sue componenti (ad esempio singoli dati, informazioni o programmi).

Ricordiamo che in tale circostanza rientrano i casi in cui questi danneggiamenti siano stati una conseguenza dell'accesso e non il mezzo agevolatore per realizzarlo, dovrà essere, in sostanza, una conseguenza non voluta (altrimenti si farebbe riferimento alla norma sul danneggiamento informatico ex art 635 bis in concorso con l'accesso abusivo).

2.4.3 RELAZIONE CON ALTRI REATI

Per quanto riguarda il concorso del reato di accesso abusivo ad un sistema informatico con altri reati si ritiene che quest'ultimo possa concorrere con quello di frode informatica ex art. 640 c.p., diversi essendo i beni giuridici tutelati e le condotte sanzionate in quanto il primo tutela il cosiddetto domicilio informatico sotto il profilo dello "ius excludendi alios" anche in relazione alle modalità che regolano

l'accesso dei soggetti eventualmente abilitati, mentre il secondo contempla e sanziona l'alterazione dei dati immagazzinati nel sistema al fine della percezione di ingiusto profitto[51].

Occorre anche analizzare il rapporto con l'art 616 c.p. "Violazione, sottrazione e soppressione di corrispondenza".

È possibile affermare che nel caso non vi sia né sottrazione né distrazione, sarà punibile solo la condotta di chi prende cognizione di corrispondenza chiusa.

Nel caso si tratti di corrispondenza "aperta" il soggetto agente risponderà penalmente soltanto per distrazione o sottrazione al destinatario.

A tal proposito importante risulta la pronuncia della Suprema Corte, la quale nega la responsabilità penale di cui all'art 616 c.p. nel caso in cui un superiore gerarchico prenda cognizione della mail contenuta nel computer del dipendente che si trova lontano dal luogo di lavoro, utilizzando una password d'accesso fornita al dipendente come da protocollo aziendale.[52]

Nel caso in esame, la password del dipendente doveva essere a conoscenza anche del suo superiore gerarchico.

Se fosse stata accertato invece un accesso abusivo, si sarebbe posta la questione della contestabilità del reato ex art 615 ter e, contestualmente, la violazione del codice della privacy nonché dell'art 4 dello Statuto dei lavoratori.

[51]Sez. 2, Sentenza n. 26604 del 29/05/2019 Ud. (dep. 17/06/2019) Rv. 276427; Sez. 5, Sentenza n. 1727 del 30/09/2008 Cc. (dep. 16/01/2009) Rv. 242938.

[52]Cass, Sez. V, 11 dicembre 2007, Proc. Rep. Trib. Torino in proc. Tramalloni

2.4.2 L'EVOLUZIONE GIURISPRUDENZIALE IN MATERIA DI ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO

La prima sentenza nella quale viene trattato il reato oggetto di studio proviene dal Tribunale di Torino, il 4 dicembre 1997; nel caso in esame si trattava di decidere in merito al coinvolgimento di alcuni dipendenti che provvisti di codici di accesso per l'utilizzo dei computer dell'impresa, provvedevano ad estrarre copia di una serie di dati contabili e fiscali per poi servirsene nelle loro singole attività imprenditoriali.
In quel contesto, il Tribunale ritenne applicabile l'art. 615 ter. c.p. nella sua forma aggravata (abuso della qualità di operatore del sistema).
Punto interessante affrontato in sentenza riguardava la possibilità di ritenere accesso abusivo quello operato da soggetti muniti di autorizzazione, anche se subordinata a determinati limiti temporali e comunque per svolgere le mansioni affidategli.
Gli imputati agivano con lo scopo di procedere alla duplicazione illegittima dei dati contenuti negli elaboratori.
I giudici sottolinearono il carattere abusivo di suddetti comportamenti.
La sentenza assume notevole importanza in quanto vengono stabiliti i principi per la teorica del "domicilio informatico", il quale rappresenta una delle possibili interpretazioni in merito al bene giuridico tutelato.

Un ulteriore tappa è rappresentata dalla sentenza n.3067 del 1999. Si trattava di un procedimento di riesame di un provvedimento cautelare, e i fatti in causa riguardavano un soggetto che si era servito del sistema

telefonico di una filiale Telecom provocando “un consistente, anomalo traffico telefonico verso l'estero” di cui avevano beneficiato due utenze estere.

La Suprema Corte si pronuncia per la prima volta sull'accesso abusivo a un sistema informatico o telematico che conferma l'orientamento del domicilio informatico, sostenuto da ragioni di carattere sistematico e sottolineando come ciò che rileva sia l'esistenza dello “ius excludendi alios”.

Tale pronuncia è notevolmente importante poiché in essa si statuisce che la tutela non va riservata solo ai casi in cui entrino in gioco contenuti personalissimi[53].

2.4.3 LA NOZIONE DI MISURA DI SICUREZZA

Dal testo normativo si evince che il reato si concreta non semplicemente a seguito dell’accesso tout court ad un sistema informatico ma richiede che tale sistema sia “protetto da misure di sicurezza”.

Giurisprudenza e dottrina ritengono che la fattispecie in esame non richieda una particolare efficacia delle misure di sicurezza adottate a salvaguardia del sistema, ma è necessaria la volontà del titolare di reprimere qualsiasi irruzione con accorgimenti tecnici, informatici e logici, anche se facilmente aggirabili.

[53] Tale orientamento giurisprudenziale si era diffuso in diverse pronunce di merito.

Ne consegue che il reato si perfeziona anche se viene violata una sola misura di sicurezza, non rilevando né il numero né, tantomeno, l'efficacia delle difese adottate dal titolare.
Dal punto di vista prettamente tecnico, le misure di sicurezza possono essere divise in due grandi categorie: misure di sicurezza digitali e misure di sicurezza non digitali.
Le prime si suddividono a loro volta tra quelle software (password, firewall) ed hardware (firma digitale o riconoscimento biometrico).
Le seconde vengono utilizzate per proteggere il sistema informatico o telematico con riguardo alla loro materialità (cassaforte, armadietto).
Le misure di sicurezza di cui all'art. 615-ter c.p. sono quelle riferibili al sistema, e non ai luoghi in cui questo viene custodito.
Di conseguenza, anche ai fini del tentativo di reato, le misure di sicurezza che dovranno risultare violate saranno quelle di tipo software e/o hardware.

2.4.4 IL PUNTO DELLA GIURISPRUDENZA SULLE MISURE DI SICUREZZA

È possibile evidenziare la presenza di due posizioni distinte da parte dei giudici nei confronti dell'elemento delle misure di sicurezza.
Una parte ritiene che la presenza di tali strumenti di protezione sia espressione dello ius excludendi alios mentre un'altra, al fine di integrare il reato, richiede il superamento delle misure di sicurezza.
La Suprema Corte con la sent. 7 novembre 2000 n.1675 e 12732 sezione V ha affermato che la norma in esame non era da considerarsi "un

illecito caratterizzato dall'effrazione dei sistemi protettivi [...] ma [...] dalla contravvenzione delle disposizioni del titolare, come avviene nel delitto di violazione di domicilio[54]

Di contro, è stato possibile concludere che integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, agisca per una finalità diversa e, quindi non rispetti le condizioni alle quali era subordinato l'accesso.

Sulla base di quanto esposto non sono mancati in dottrina degli interventi volti a sottolineare una certa contradditorietà nelle pronunce della Suprema Corte dato che si dava rilevanza al momento finalistico perseguito dall'agente[55].

Successivamente il Tribunale di Roma in data 4 aprile 2000, enuncia un principio di diritto secondo il quale al fine del perfezionamento della fattispecie criminosa vengono richiesti dei mezzi efficaci di protezione dal titolare del sistema, nonché deve essere portato a compimento un "effettiva effrazione" al fine del perfezionamento del reato di cui all'art 615 ter c.p.

[54]Cass., Sez. V, 7 novembre 2000, n.12732, in Cass. Pen.,2002,3,1018
[55]G. ARONICA, *op.cit.,* p.214

2.4.5 SOLUZIONI DOTTRINARIE SUI BENI GIURIDICI TUTELATI

La Raccomandazione Europea ha instaurato una stretta correlazione, tra il domicilio fisico e quello virtuale in modo che quest'ultimo fosse qualificato, nel nostro ordinamento, non come nuovo ed autonomo interesse, ma come risultato dell'estensione del campo semantico del "domicilio" ex art. 14 Cost.

Tale scelta risulta conforme a quell'orientamento dottrinale secondo il quale i diritti sanciti dal testo costituzionale farebbero parte di una serie "chiusa" e, dunque, tassativa, rispetto alla quale l'art. 2 Cost. svolge esclusivamente una funzione riassuntiva: pertanto, non sarebbe possibile, come da altri sostenuto[56], individuare, per mezzo dell'art. 2 Cost., nuovi diritti fondamentali, ma soltanto operare un'interpretazione estensiva delle sin- gole disposizioni costituzionali, al fine di individuare interessi comunque derivanti da quelli espressamente riconosciuti[57].

Qualora, si rinvenga il referente normativo del domicilio informatico non nel testo costituzionale, ma nel diritto sovranazionale, l'estensione dell'ambito applicativo del "domicilio" ex art. 14 Cost. potrebbe essere operata per mezzo del combinato disposto dell'art. 117, c. 1 Cost. con gli artt. 8 CEDU e 7 CDFUE, i quali sanciscono il più ampio diritto alla "riservatezza".

---

[56]V. in tal senso *A. BARBERA*, Art. 2, in *Commentario della Costituzione, Principi fondamentali* (artt. 1-12), a cura di G. Branca, Zanichelli, Bologna, 19

[57]V. in tal senso A. BALDASSARRE, Diritti inviolabili, in Enc. Giur., vol. XI, Treccani, Roma, 1989, p. 5 ss., ora in ID., Diritti della persona e valori costituzionali, Giappichelli, Torino, 1997, p. 61.

Le disposizioni sovranazionali costituirebbero, secondo questa opzione, una «sintesi in funzione di sviluppo» dei diritti sanciti dagli artt. 13, 14 e 15 Cost., tale da consentirne una «massimizzazione delle tutele»[58].

Entrambi i percorsi appena descritti conducono al medesimo risultato estensivo del domicilio fisico, ma non tengono conto delle peculiarità che caratterizzano i reati informatici, le quali riflettono «la diversa struttura dei rapporti (anche illeciti) che si svolgono, in tutto o in parte, nel Cyberspace» e che valgono a distinguerli dalle fattispecie "classiche" alle quali sono accostati[59].

La rilevanza dello spazio digitale, per quanto centrale nella società contemporanea, non sembra in alcun modo equiparabile al valore che, fin dall'antichità, l'individuo attribuisce al proprio domicilio ed alla pace domestica.

Rispetto ai problemi sopra delineati, la dottrina ha individuato un nuovo bene giuridico rappresentato dalla "riservatezza informatica" ed enucleato per mezzo dell'art. 2 Cost. (qualificato come fattispecie "aperta" e con funzione espansiva dei diritti costituzionali) o dell'art. 117, c. 1 Cost., in quest'ultimo caso con l'intermediazione delle disposizioni sovranazionali che tutelano il rispetto della vita privata (8 CEDU e 7 CDFUE)[60].

---

[58]G. SILVESTRI, *L'individuazione dei diritti della persona*, in www.penalecontemporaneo.it, 29 otto- bre 2018, p.

[59]L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in Trattato di Diritto penale – Cybercrime, cit., p. 75.

[60]C. DOMENICALI, *Tutela della persona negli spazi virtuali: la strada del "domicilio informatico"*, in www.federalismi.it, 28 marzo 2018, p. 8.

Al fine di superare i dubbi interpretativi che, come visto, discendono dalla qualificazione dell'interesse protetto come "domicilio informatico" o "riservatezza informatica", una parte della dottrina esclude che l'elaboratore o il sistema telematico presentino necessariamente quella connotazione personale che deve pur sempre caratterizzare il diritto alla riservatezza ed il domicilio, ed individuano il bene giuridico tutelato del reato nella "intangibilità informatica", ossia nello ius excludendi alios che fa capo al titolare del sistema[61].

2.4.6 LE MODALITA' DI AGGRESSIONE INFORMATICA

Le modalità di attacco informatico possono essere divise in due categorie: 1) le tecniche di monitoraggio, strumentali all'attacco informatico;
2) i veri e propri attacchi informatici.
Un esempio di attacco riguardante la prima categoria è rappresentato dallo "***spoofing***" con il quale viene virtualmente sostituito il proprio computer in rete grazie all'utilizzo di informazioni identificative (quali l'IP e l'*hostname*) realizzando una sorta di "sostituzione di identità tra sistemi informatici.
Un ulteriore modalità di attacco prende il nome di "***port scanning***", con il quale viene effettuata una verifica di tutte le porte di connessioni

[61] V. in tal senso: V. MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. eco*., 1992, p. 374 ss.; L. PICOTTI, *Reati informatici, in Enc. Giur.*, Agg., 2000, p. 20 ss.

attive su un sistema in rete, al fine di individuare le porte prive di protezione *firewall.*

Infine, va menzionato anche lo ***sniffing***, ovvero l'ascolto della comunicazione tra due sistemi in modo da intercettarne i pacchetti in entrata e in uscita, con tale mezzo il soggetto può entrare in possesso di una moltitudine di dati, quali: il contenuto di messaggi, password di siti web, credenziali bancarie.

Rientrano nell'annovero dei veri e propri attacchi *Cibernetici,* il ***backdoor*** per mezzo del quale il soggetto agente riesce ad ottenere il pieno accesso al pc della vittima, e così utilizzarlo a scopi criminali.

Importante è l'utilizzo dei c.d. spyware, oramai diffusi addirittura più dei virus.

Non sono altro che software, o chiavi di registro che si installano nel sistema senza che l'utente ne sia a conoscenza.

Come suggerisce il nome, sono dei software-spia che hanno la funzione di trasmettere contenuti del sistema della vittima al computer dell'autore dell'attacco informatico.

L'applicazione più diffusa è quella di leggere il contenuto dei cookies e di catalogarli in modo da tracciare un profilo delle attività di navigazione svolte.

SEZIONE QUINTA

(LA TUTELA PREVENTIVA DEI SISTEMI INFORMATICI)

2.5 La tutela anticipata in materia di reati informatici

2.5.1 Dai delitti di attentato alle norme di cd. sbarramento

Prima di analizzare in dettaglio le due norme, in tema di reati informatici riconducibili alle categorie delle norme di "sbarramento" di cui agli artt. 635 quater e art. 635 quinquies c.p., occorre individuare le finalità dei reati di attentato, nonché andare ad analizzare i numerosi problemi di legittimità costituzionale che sono stati sollevati nel corso del tempo, poiché vi è il rischio di accantonare il principio di offensività.

In gran parte della dottrina, ma anche nel panorama giurisprudenziale, viene richiesto il requisito di offensività oltre a all'idoneità degli atti.

Al fine di evitare il rischio di allontanarsi dal principio di necessaria offensività, è almeno richiesto che la struttura dei delitti di attentato sia simile alla struttura dei reati che prevedono il tentativo.

L'idoneità degli atti svolge pertanto un ruolo importantissimo, il problema si pone infatti nei giudizi al riguardo.

Il pensiero giurisprudenziale ha mutato il proprio orientamento nel corso del tempo; un tempo, richiedeva la "mera possibilità" del verificarsi dell'effetto dannoso, per poi mutare orientamento alla teoria della "non impossibilita" del verificarsi dell'evento.

Il problema di queste teorie risiede nella estensione conseguente dell'ambito applicativo a tutta la serie di atti di natura preparatoria non costituenti un pericolo per l'oggetto di tutela.
La soluzione è costituita dal prendere in considerazione solo quegli atti rappresentativi di un pericolo concreto che in un'ottica di probabilità o possibilità risulta suscettibile di mutarsi in danno.
Pertanto, è tutt'altro che scontata la portata tipizzatrice del requisito della idoneità, che stenta ad essere considerata come dotata di "una efficacia determinativa della tipicità delle condotte a forma libera".[62]
Il concetto sopra menzionato svolge la funzione di rapportare l'evento e la condotta.
È richiesto che l'evento sia descritto puntualmente; inoltre, lo stesso dovrà essere leggibile anche in termini di offensività.
In base a tale previsione sono state individuate, nell'annovero dei reati di attentato, tre insiemi caratterizzati dalla diversa formulazione degli eventi.
Grazie a ciò sarà possibile riconoscere quel gruppo di reati connotati da eventi privi di un connotato offensivo intrinseco e, di contro, sarà possibile individuare un gruppo di reati che preannunciano eventi dal risultato "ultra lesivo" ed infine quelle fattispecie che hanno una funzione prettamente anticipatoria della tutela.
Proprio in tali fattispecie è possibile individuare le c.d. norme di sbarramento in tema di reati informatici degli art. 635 ter e 635 quinquies c.p.

[62]I.SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, *Rivista di dir. e proc. penale*, p. 225

Bisognerebbe, a sua volta, distinguere le ipotesi nelle quali il risultato in relazione al quale l'azione è diretta fa riferimento non ad eventi compiuti, ma a degli sviluppi ulteriori di carattere complesso, da quelli dove invece appare possibile (anzi indispensabile) una prognosi postuma.

Con riferimento a questi ultimi, devono rispondere all'idoneità ed univocità, alla pari di quanto avviene nel contesto delle ipotesi di tentativo dei corrispondenti delitti-base.

I reati citati sono connotati da un elemento di specialità con i tentativi di reati di danneggiamento di informazioni di dati e programmi di cui all'art 635 c.1 c. p e danneggiamento di sistemi informatici e telematici ex art. 635 quater c.1 c.p.

Dovrà essere fatto una prognosi ex ante per verificare se gli atti risultano idonei sotto il punto di vista oggettivo, nonché diretti in modo non equivoco a produrre un particolare pericolo al bene giuridico oggetto di tutela.

La ratio di approntare una risposta sanzionatoria equivalente a quella del reato consumato è data da una scelta politico criminale poiché se al fatto-reato venisse applicata la disciplina del tentativo, il risultato potrebbe apparire non raggiungibile.

Accanto a questa ratio, esiste anche quella dovuta alla stessa ontologia del fatto sanzionato.

Se venisse raggiunto lo scopo cui è indirizzata la volontà del reo, la conseguenza potrebbe essere quella dell'impunità per lo stesso.

Esempi paradigmatici sono rappresentati da tutti i reati contro la personalità dello Stato: se lo scopo, ad esempio, della menomazione

dell'unità dello Stato venisse concretamente raggiunto, l'assetto istituzionale verrebbe gravemente compromesso. Con riguardo alle due fattispecie in esame la domanda da porsi è se sussista uno di questi presupposti che diano una giustificazione al loro inserimento. Per parte della dottrina la risposta è negativa non essendo riscontrabile una particolare esigenza deterrente né tanto meno un pericolo per l'impianto politico-istituzionale dello Stato.[63]

2.5.2 NORME DI SBARRAMENTO: CARATTERISTICHE FINALITÀ; TIPOLOGIE DI SOFTWARE "DANNOSO"

In dottrina, è stata esplicata la presenza di una sottocategoria di reati informatici, caratterizzata da una anticipazione della tutela.
Trattasi di due norme volte a prevenire e a sanzionare condotte di carattere prodromico rispetto a quelle descritte negli altri reati informatici.
L''art. 615 quater c.p., punisce l'abusiva acquisizione e diffusione di mezzi o codici di accesso ad un sistema informatico o telematico protetto da misure di sicurezza, e l'art. 615 quinquies c.p. che sanziona la diffusione di apparecchiature, dispositivi e programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.

[63]I.SALVADORI, *op.cit*., p. 229

La finalità preventiva presente in ambedue le fattispecie, è rinvenibile allo stesso tempo in una differenza cui va ad esplicarsi il fine anticipatorio di tutela.

La disposizione di cui all'art. 615 quater c.p. è facilmente ricollegabile alla fattispecie di accesso abusivo ad un sistema informatico o telematico ex art. 615 ter c.p. Infatti, essa mira a prevenire proprio l'accesso sanzionando condotte di coloro i quali siano in possesso di parole chiave(password), codici ovvero qualsiasi altro mezzo atto a consentire l'accesso non autorizzato ad un sistema informatico o telematico protetto da misure di sicurezza.

È chiaro presumere che la disciplina normativa in esame sia legata anche alla fattispecie di frode informatica ex art. 640 ter c.p.: non solo non viene richiesto il conseguimento del profitto nella acquisizione e diffusione di mezzi atti ad accedere abusivamente nel sistema, ma è innegabile che le condotte descritte nel 615 quater siano adottate anche da chi si trova nell'intento di commettere una frode informatica.

Invece, La norma di cui all'art. 615 quinquies c.p. è specificatamente rivolta a prevenire il danneggiamento del sistema informatico o telematico.

Infatti, è richiesto il dolo specifico che rapportato al contenuto della norma deve essere diretta a danneggiare e/o provocare un'alterazione e/o un'interruzione di un sistema informatico o telematico.

I principali "*software*" idonei a far raggiungere tale intento criminoso sono i *virus informatici;* ovvero un software appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da fare copie di sé stesso, generalmente senza farsi rilevare dall'utente.

I *virus* svolgono una serie di operazioni impartite dallo sviluppatore, inoltre, al fine da risultare quasi "invisibili" occupano una quantità di risorse di sistema pressoché irrisoria, in modo da agire indisturbati all'interno del sistema della vittima.

Esistono numerose tipologie di virus informatici, tra i quali i c.d. trojan, tale tipologia di virus non si replica all'interno del sistema, bensì si cela dietro dei comuni software, sono software alquanto dannosi in quanto danneggiano parti del *sofware* di sistema ovvero rendono accessibile la macchina a terzi.

Un ulteriore tipologia di virus è rappresentata dai "*worms*" poiché si diffondono senza il bisogno di alcun programma ospite.

I *Logic Bombs* invece si attivano dopo un determinato arco di tempo la loro istallazione; invece, gli *spyware* come afferma la parola stessa, forniscono informazioni sulle attività della vittima.

2.5.3 LA DETENZIONE E DIFFUSIONE DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI

La norma è collocata nel Libro II – dei Delitti in particolare, titolo XII– dei Delitti contro la persona, Capo III – dei delitti contro la libertà individuale, Sezione IV dei delitti contro la inviolabilità del domicilio.

L'articolo è stato aggiunto dall'art. 4, l. 23.12.1993, n. 547.

La natura giuridica è quella di reato comune, di pericolo, di mera condotta, a forma vincolata.

Quanto alla ratio della norma ed alla natura giuridica del reato, è sanzionata l'abusiva acquisizione e diffusione, con qualsiasi modalità,

dei mezzi o codici di accesso preordinati a consentire a soggetti non legittimati l'introduzione nel sistema informatico o telematico altrui protetto da misure di sicurezza.

La finalità è quella della repressione di condotte prodromiche alla realizzazione del delitto ex art. 615-ter c.p. e, nella specie, di una particolare ipotesi connotata e qualificata dalla sostituzione illegittima dell'agente al titolare del sistema mediante l'uso della password di quest'ultimo.

È configurato quale "reato ostativo", poiché finalizzato ad evitare il compimento di più gravi delitti contro la riservatezza o contro il patrimonio.

Sul bene giuridico tutelato dalla norma esistono diverse tesi contrapposte.

Secondo una prima tesi si tratta di anticipare la tutela del domicilio informatico; secondo una seconda tesi, l'obiettività giuridica è da identificarsi nel rafforzamento della tutela della segretezza dei dati e dei programmi contenuti in un elaboratore; inoltre, secondo una terza tesi, la noma esprime una tutela anticipata più ampia dei beni giuridici potetti da una serie di norme penali informatiche (patrimonio, riservatezza, fede pubblica) col fine di prevenire, in via generale, la commissione dei reati informatici; secondo una quarta tesi, oggetto di tutela è la prevenzione degli accessi abusivi effettuati senza alterazione del software di protezione del sistema e mediante la sostituzione illegittima del titolare dell'accesso nell'uso della password.

L’oggetto materiale della condotta incriminata sono i «codici», le «parole chiave» o gli «altri mezzi idonei all’accesso» ad un sistema informatico o telematico che sia protetto da misure di sicurezza.

Il «codice di accesso (o parola chiave)», è la chiave che permette di collegarsi logicamente al sistema.

può trattarsi di sequenza alfabetiche, numeriche o alfanumeriche o numero-logiche che, se digitate alla tastiera o altrimenti comunicate all’elaboratore (es. attraverso un microfono o un lettore ottico), consentono l’accesso ai dati ed ai programmi contenuti nella memoria interna; «qualsiasi mezzo idoneo all’accesso», sono i mezzi di accesso fisici (chiavi meccaniche, chiavi elettroniche e cioè tesserini magnetici di riconoscimento, carte di credito, ecc.…); mezzi logici (parole chiave nel senso di password ovvero i mezzi che consentono di collegarsi logicamente al sistema); indicazioni o istruzioni idonee a realizzare un accesso abusivo (le informazioni tecniche riservate che non svelano il codice di accesso, ma il metodo idoneo a raggiungere lo scopo).

Le condotte sanzionate penalmente consistono, alternativamente, nell’ «acquisire» i mezzi necessari per accedere al sistema informatico altrui, indipendentemente dalle modalità di acquisizione; nel «procurare» ad altri codici, parole chiavi o altri mezzi idonei a consentire l'accesso abusivo; nel «diffondere», «comunicare» o «consegnare» a terzi detti mezzi (sia per iscritto che oralmente); nel «fornire» le informazioni, indicazioni, istruzioni idonee a consentire l'accesso ad un sistema informatico altrui protetto da misure di sicurezza; la «detenzione», invece, indicata nella dizione della rubrica ma non nel contenuto della disposizione, per taluni è ricompresa nella nozione di «procurarsi».

Il reato si consuma nel momento e nel luogo in cui si realizza la condotta tipica e, quindi, allorché il soggetto agente acquisisca la disponibilità del codice di accesso entrando materialmente in possesso di esso, o pervenendo autonomamente alla sua individuazione, ovvero nel momento in cui viene compiuto il primo atto di diffusione o si realizza la comunicazione o la consegna a terzi di tali mezzi o di informazioni sul modo di eludere le barriere di protezione di un sistema informatico.

Infine, va ricordato anche che l'applicabilità della norma interessa anche i sistemi di natura telematica.

Ciò ha portato al ricorso al 615 quater nei casi di ottenimento del numero di serie di un apparecchio di telefonia mobile, appartenente ad altri e alla conseguente "clonazione" tale da consentire la connessione alla rete mobile a spese altrui.

Rientrano anche gli ormai diffusissimi casi di "Card-Sharing", con la quale viene fornito il servizio pirata c.d. "IPTV" metodo per mezzo del quale, un abbonamento alla "pay tv" viene condiviso con una serie indefinita di soggetti con lo scopo di non pagare il relativo canone, o pagarlo ad un prezzo irrisorio.

Queste condotte non sono certo prive di una copertura penalistica data l'esistenza della norma di cui all'art. 171 octies l.22 aprile 1941 n.633 sul diritto d'autore, il quale è stato rivisitato con le successive modifiche apportate con la legge 248 del 18 luglio 2000, con il D.Lgs. 9 aprile 2003 n. 68, con il D.L. 22 marzo 2004 n. 72, con il D.L. 31 gennaio 2005 n.7, con il D.Lgs. 15 febbraio 2006 n. 118 e con il D.Lgs. 16 marzo 2006 n. 140.

Inoltre, il reato consistente nell'utilizzo indebito di carte di credito o similari strumenti di pagamento e prelievo, disciplinato dall'art. 55 d.lgs. 21 novembre 2007 n.231, è stato ritenuto integrato nei casi di ricariche telefoniche effettuate con codici sottratti, escludendo l'applicabilità dell'art. 615 quater c.p.

L'elemento soggettivo consiste nel dolo specifico richiedendosi la finalità di agire "al fine di procurare a sé o ad altri un profitto arrecare ad altri danno".

Il secondo comma, nel prevedere le circostanze aggravanti richiama quelle relative ai numeri 1) e 2) dell'art. 617 quater c.4 c.p.: sono il caso in cui i sistemi informatici o telematici in questione siano utilizzati dallo Stato o da altro ente pubblico o da impresa esercente.

Il tentativo non è configurabile alla luce della sua natura giuridica di reato di pericolo astratto, a causa dell'eccessivo arretramento della tutela penale che ne deriverebbe.

L'elemento soggettivo è il dolo specifico, ovverosia coscienza e volontà di procurarsi, riprodurre, diffondere e comunicare codici di accesso o mezzi similari al fine di procurare a sé od altri un profitto o di arrecare ad altri un danno.

Le circostanze aggravanti sono ad effetto speciale (aumento di pena superiore ad un terzo della pena base); sono agganciate o all'abuso da parte dell'agente di una particolare posizione funzionale oppure alla particolare importanza e delicatezza del sistema informatico o telematico coinvolto.

Quanto al rapporto dell'art. 615-quater c.p. con l'at. 615-ter c.p., le due previsioni non concorrono, prevedendo l'art. 615-quater c.p. condotte prodromiche all'illecito ex art. 615-ter c.p.[64]

2.5.4 DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO, *EX* ART. 615-*QUINQUIES* C.P.

L'articolo è stato prima aggiunto dall'art. 4, L. 23.12.1993, n. 547, e successivamente così modificato dall'art. 4, L. 18.3.2008, n. 48 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica).

La Riforma del 2008 estende la protezione contro una più ampia gamma di fonti di rischio, non solo i software infetti (Virus informatici), ma anche gli hardware infetti (apparecchiature e dispositivi informatici) diretti a danneggiare o interrompere un sistema informatico o telematico; amplia le condotte sanzionate e prevede che quella che costituiva la caratteristica intrinseca delle fonti di rischio, vale a dire lo scopo o l'effetto di danneggiare, rappresenti (anche) il fine perseguito dal soggetto agente con la sua condotta.

Per tale tipologia di fattispecie, la rilevanza penale sussiste anche qualora non si verifichi il danneggiamento informatico, in quanto si tratta di un reato di pericolo astratto.

[64] AVV. FRANCESCO ALBANESE E AVV. VALENTINA PRIVITERA *op.cit.*, pag. 14-16

Prima della riforma del 2008, era richiesto quale elemento psicologico il dolo generico ma ciò creava non pochi problemi riguardanti il non sempre facile riscontro in concreto della rilevanza penale di determinate condotte.
La convenzione inoltre, richiedeva la previsione di una soglia minima di apparecchiature, all'interno della nozione "procurarsi", ma il legislatore non ha seguito tale indicazione non comportando però ciò, l'impossibilità di valutare il dolo specifico in presenza di un ingente numero di apparecchiature procurate.[65]

SEZIONE SESTA

(La tutela della La tutela della libertà e riservatezza delle comunicazioni)

2.6 INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

2.6.1 BENE GIURIDICO OGGETTO DI TUTELA

L'art. 617 quater, introdotto dalla l. 547 1993, sanziona penalmente *chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa, venendo punito con la reclusione da sei mesi a quattro anni.*

[65]C.SANTORIELLO E AA.VV., *op.cit.,* p.99

In*oltre è soggetto alla stessa pena, salvo che il fatto costituisca un più grave reato, chiunque riveli, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle predette comunicazioni.*

Era già prevista nel sistema codicistico una norma a tutela delle intercettazioni di comunicazioni o conversazioni telematiche o telegrafiche all'art 617 e ss. c.p.

Il legislatore avrebbe potuto ampliare la portata dell'art 623 bis c.p., ma ha optato per una scelta differente, ovvero, introdurre nuove fattispecie incriminatrici in particolare gli art.617 quater (intercettazione, impedimento, o interruzione di comunicazioni informatiche o telematiche) e l'art 617 quinques c.p. (installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche).

Il bene giuridico oggetto della tutela penale consiste nella libertà e riservatezza delle comunicazioni; ciò è quanto affermato dalla dottrina maggioritaria.

Le comunicazioni che trovano tutela negli articoli oggetto di esame sono quelle in fase di trasmissione.

Per quanto riguarda la comunicazione intesa in senso statico è infatti prevista una norma, ossia l'art 616 c.p. (Violazione, sottrazione e soppressione di corrispondenza).[66]

Pertanto, al fine di rendere più chiaro il concetto in esame, l'art. 617 quater andrebbe a tutelare il profilo dinamico della corrispondenza, i

[66]F. TAVASSI LA GRECA, *Hacking e criminalità informatica*, *www.altrodiritto.unifi.it*

caratteri principali sono infatti quelli della personalità e attualità della conversazione.
Le varie modalità di comunicazione simultanea come le chat line, la videoconferenza, che consente in tempo reale lo scambio e la condivisione di documenti, immagini, suoni.
Date queste considerazioni, ne consegue che la presa di cognizione di una conversazione cristallizzata in un qualsiasi supporto fisico (cd-rom, hard disk etc.) rientrerà nell'ambito applicativo dell'art. 616 c.p. mentre la captazione della conversazione in atto integra l'art. 617 quater c.p.

2.6.2 LE CONDOTTE DI "INTERCETTAZIONE", "INTERRUZIONE", "IMPEDIMENTO", "RIVELAZIONE"

Per quanto riguarda la condotta di «intercettazione», si intende la presa di cognizione che si realizza attraverso la modalità della intromissione nella comunicazione in corso tra terzi, in cui il soggetto captante non è anche conversante.
Essa deve avere ad oggetto il contenuto di una comunicazione informatica o telematica in atto, nel momento dinamico della sua trasmissione.
Interessante è la lettura interpretativa da attribuire al termine "fraudolentemente", chiedendoci se debba essere riferito indistintamente alla intercettazione, ovvero, alle altre due condotte, oppure, se si debba considerare solo con riguardo alla prima.

A sostegno di quest'ultima teoria bisogna considerare due elementi: il primo è rappresentato dalla lettera della norma dalla quale, in maniera non certo ambigua, si evince che l'avverbio vada riferito solo all'intercettazione, il secondo verte sulle conseguenze che la lettura alternativa avrebbe: ne conseguirebbe infatti l'estromissione *"dall'ambito di operatività della norma le ipotesi di impedimento e interruzione di comunicazioni in atto realizzate in modo violento anziché fraudolento"*.[67]

Da sottolineare come la fraudolenza è da intendersi come "modalità occulta di attuazione dell'intercettazione"[68] ; si può pertanto affermare l'esclusione dell'applicabilità della norma qualora l'intercettato sia a conoscenza, in maniera non casuale, antecedentemente all'inizio della conversazione della condotta altrui.

L'«interruzione» e l'«impedimento» consistono nel compimento di atti tecnicamente idonei, da un lato, a far cessare una comunicazione in corso e, dall'altro, ad impedire che una nuova comunicazione abbia inizio (es. utilizzo di un software che causi lo spegnimento del modem di chi sta navigando in internet con l'interruzione della comunicazione in corso).

La «rivelazione» al pubblico si verifica qualora, l'agente, ha in qualsiasi modo - anche per via occasionale, o perfino con l'assenso dei dialoganti - acquisito la conoscenza del contenuto di una "comunicazione in atto", e poi ne renda pubblico il relativo contenuto.

[67]C. PECORELLA, *Il diritto penale dell'informatica*, p. 304
[68]F. TAVASSI LA GRECA, *op.cit.*

2.6.3 ELEMENTO SOGGETTIVO

Sotto il punto di vista soggettivo è richiesta la presenza del dolo generico, consistente nella rappresentazione e volontà del fatto tipico nel suo complesso. Quindi sarà necessario e sufficiente che l'agente sia consapevole e voglia tenere le condotte di intercettazione fraudolenta, interruzione o impedimento delle comunicazioni intercorrenti tra due sistemi informatici o telematici o provenienti da un sistema informatico o telematico oppure di rivelazione, tramite qualsiasi mezzo di informazione al pubblico, il contenuto totale o parziale delle stesse.

2.6.4 LE CIRCOSTANZE AGGRAVANTI

Le circostante aggravanti del reato sono circostanze ad effetto speciale; il particolare disvalore è identificato dal fatto che il reato è commesso in danno di un sistema informatico o telematico utilizzato dallo stato da altro ente pubblico o da impresa esercente servizio di pubblica necessità, o da un soggetto con una particolare qualifica (pubblico ufficiale o incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o con abuso della qualità di operatore del sistema o esercente anche abusivamente, la professione di investigatore privato); operatore di sistema è colui che controlla il processo di ricezione, elaborazione e diffusione dei dati, potendo influire sulla loro destinazione o integrità.

2.6.5 ART 617 QUINQUES C.P. L'INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE COMUNICAZIONI INFORMATICHE O TELEMATICHE.

Tale norma rientra tra quelle appartenenti alla categoria dei reati che offrono una tutela anticipata (nell'ambito dei reati informatici).
Importante sottolineare come, al fine dell'integrazione della fattispecie criminosa, non sia richiesto il successivo funzionamento delle apparecchiature; sarà però compito del giudice verificare l'idoneità degli strumenti al raggiungimento dello scopo criminoso.
Occorre al fine di inquadrare la fattispecie in esame, menzionare il punto di diritto della Suprema Corte la quale afferma: «*integra il delitto ex art. 617-quinquies c.p. la condotta di colui che installa abusivamente apparecchiature atte ad intercettare comunicazioni relative ad un sistema informatico posizionando nel «postamat» di un ufficio postale una fotocamera digitale, considerato che, l'intercettazione, implica che l'agente si inserisca nelle comunicazioni riservate, traendo indebita conoscenza delle stesse.*»[69]
Si può ben notare, dalla pronuncia della Suprema Corte, come gli strumenti fossero idonei a far presumere il raggiungimento dello scopo criminoso, elemento richiesto ai fini della configurabilità del reato ex.art 617 quinques c.p.

[69]CORTE DI CASSAZIONE, SEZ. 5, 30.1.2007, N. 3252

2.6.6 ART. 617 SEXIES C.P: LA FALSIFICAZIONE, ALTERAZIONE O SOPPRESSIONE DEL CONTENUTO DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

L'art 617 sexies c.p prevede: «*colui che, 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.*»

Con la già criticata ripetizione di previsioni penali, il legislatore del 1993 ha ritenuto di dover introdurre una specifica e nuova incriminazione anche per punire la falsificazione, alterazione o soppressione del contenuto di "comunicazioni informatiche o telematiche".

In tale scelta appare evidente, ed è del resto dichiarato[70], il condizionamento del modello delineato dalla precedente novella di cui alla l. n. 98 del 1974 che, apprestato dai "nuovi" artt. 617 e 617 *bis* c.p. alla libertà e riservatezza delle "comunicazioni telegrafiche e

[70] Cfr. la Relazione ministeriale al d.d.l. n. 2773, pag. 10, che a proposito degli artt. 617 *quater*, 617 *quinquies* e 617 *sexies* c.p., introdotti tutti dall'art. 6, parla semplicemente di "estensione" della tutela prevista dal codice per le comunicazioni telefoniche o telegrafiche "a quelle informatiche o telematiche", senza nulla aggiungere di specifico al riguardo, oltre alla parafrasi delle norme stesse.

telefoniche", ha inserito la specifica normativa dell'art. 617 *ter* c.p. per tutelarne anche la sicurezza ed integrità, relativamente alla loro genuinità e veridicità[71].

Dopo aver, quindi, sanzionato la predisposizione di apparecchiature idonee ad intercettare, interrompere o impedire comunicazioni attinenti a sistemi informatici o telematici (art. 617 *quinquies* c.p.), nonché il loro impiego e la rivelazione al pubblico dei contenuti (art. 617 *sexies* c.p.), il legislatore si è occupato del caso in cui, verificatasi un'intercettazione, l'operatore disponga della comunicazione così acquisita, falsificandola, alterandola o sopprimendola e ne faccia o consenta poi l'uso per scopi di profitto o di danno altrui.[72]

---

[71] L. MONACO, in Crespi, Stella, Zuccalà (a cura di), *Commentario breve al Codice penale*, I ed., 1992, pag. 1425, *sub* art. 617 *ter*; Antolisei, cit., pag. 250; Marini, *Reati contro la persona*, cit., pagg. 419 e 429; Pica, *op. cit.*, pag. 419; Fondaroli, *op. cit.*, pag. 317.

[72] ANTOLISEI, *Manuale di diritto penale parte speciale.*, pag. 251.

CAPITOLO TERZO
3.0 LA CONFISCA NEI REATI INFORMATICI

3.1 LA CONFISCA NEI REATI INFORMATICI: LE NORME INTRODOTTE

Il dilagante fenomeno dei reati *cybernetici* ha portato il legislatore ad alzare il grado di tutela, prevedendo per determinate tipologie di fattispecie criminose commesse per mezzo di strumenti informatici, l'istituto della confisca.

Con la legge 15 febbraio 2012, n.12 sono state introdotte alcune nuove disposizioni in materia di confisca dei beni informatici e telematici utilizzati per la commissione di reati informatici e di destinazione dei medesimi beni.

In particolare, l'art. 1 della novella modifica l'art. 240 cod. pen., configurando nel secondo comma del medesimo, al numero 1-*bis*, una nuova ipotesi di confisca obbligatoria relativa ai beni e agli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati informatici previsti dal codice penale e cioè dei reati di

- accesso abusivo ad un sistema informatico o telematico (art. 615-*ter*);
- detenzione e diffusione abusiva di codici di accesso ai sistemi informatici o telematici (art. 615-*quater*);
- diffusione di apparecchiature, dispositivi o programmi informatici

diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies);

- installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-*bis*);
- falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche (art. 617-*ter*);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater*);
- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies);
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 617-*sexies*);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis*);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter*);
- danneggiamento di sistemi informatici e telematici, anche di pubblica utilità (artt. 635- *quater* e 635-quinquies)
- frode informatica (art. 640-*ter*)
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies).

Oggetto di modifica anche il terzo comma del citato art. 240, dove è stato precisato che l'obbligo di confisca non opera in caso in cui la cosa o il bene ovvero «lo strumento informatico o telematico» appartiene a

persona estranea al reato anche in riferimento alla nuova ipotesi di ablazione introdotta al comma 1-*bis*.

Ed in proposito vale la pena evidenziare come in dottrina è stato criticato il probabile eccesso classificatorio in cui è caduto il legislatore nell'aver voluto a tutti i costi distinguere gli «strumenti informatici» dai beni e dalle cose oggetto di confisca, quasi si trattasse di entità fisiche non rapportabili al genus «cose».

Peraltro, nel terzo comma dell'art. 240 cod. pen. è stato altresì aggiunto un periodo in cui si stabilisce che, sempre nell'ipotesi di cui al n. 1-*bis* di nuova introduzione, si procede alla confisca obbligatoria anche nel caso di patteggiamento.

L'articolo 2 della novella introduce invece nelle disposizioni di attuazione del codice di procedura penale l'inedito art. 86-*bis*, mediante il quale è disciplinato l'impiego e la destinazione dei beni e strumenti informatici utilizzati per la commissione dei reati informatici e di quelli di cui agli artt. 473 e 474 cod. pen. ed oggetto di provvedimento di sequestro o di confisca. In particolare, il primo comma del nuovo articolo prevede che i beni o strumenti informatici o telematici, i quali a seguito di «analisi tecnica forense» risultano essere stati utilizzati per commettere uno dei reati indicati in precedenza, se sequestrati vengano affidati in custodia giudiziale con facoltà d'uso, salvo che vi ostino «esigenze processuali», agli organi di polizia che ne facciano richiesta al fine di impiego nel contrasto alla criminalità informatica, ovvero ad

altri organi dello Stato che li utilizzano comunque per finalità di giustizia. [73]

3.2 BENI E STRUMENTI OGGETTO DI CONFISCA

Occorre andare a delineare quali categorie di "beni" o "strumenti" previsti dalla legge n. 12 del 25 febbraio 2012, possono essere oggetto di confisca.

A tal proposito occorre darne una nuova definizione: quali oggetti legati alle condotte tipiche dei reati informatici da vincolo pertinenziale e funzionale; *"Il bene (informatico o telematico) assumerebbe perciò il significato di un oggetto − la cui valutazione è apprezzabile e manifesta − il quale sia direttamente utilizzato nelle condotte di reato previste dalla legge nel senso che tramite il suo uso viene ad essere conseguito il profitto del reato, e mediante la sua (accertabile) organizzazione, anche articolata e complessa, condiziona il risultato criminoso nel suo insieme".* [74]

Quanto attiene alla nozione di strumento, "*deve ricollegarsi alla realizzazione materiale della condotta criminosa accertata mediante un vincolo funzionale e tecnologico, e che consiste nella fruizione*

[73] LUCA PISTORELLI*, novità legislative* – l. febbraio 2012,, recante *"Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica" – Disposizioni rilevanti per il settore penale.*
[74] GIUSEPPE CORASANITI*, Brevi note in tema di confisca obbligatoria di "beni e strumenti" di commissione dei reati informatici alla luce della legge 15 febbraio 2012, n. 12, Dir. informatica*, fasc.4-5, 2012, pag. 819

dell'oggetto (o dell'insieme di oggetti) al fine di conseguire un determinato risultato".[75]

Alla luce di ciò appare pacifico come gli "strumenti" e i "beni" debbano avere una connotazione informatica o telematica, nonché, utilizzati dal soggetto agente al compimento della condotta criminosa.

Tramite tale assunto è possibile inserire in tali categorie, qualsiasi "oggetto" che rientra in astratto nel presente schema normativo, il quale comporta il sequestro nel caso in cui venga accertata la commissione di reati informatici tramite il loro utilizzo.

3.3 LE CRITICITÀ IN DOTTRINA RIGUARDO LA CONFISCA OBBLIGATORIA

Sono molte le critiche riguardanti la novella legislativa in materia di sequestro di beni o strumenti informatici o telematici.

La dottrina afferma che:" *L'aver eccessivamente allargato la nozione di oggetti destinati alla commissione del reato, comporta il rischio di appesantire gli uffici giudiziari e di polizia inserendo disposizioni siffatte*"

Un ulteriore nota dolente è da ravvisarsi nell'ampliamento della punibilità delle condotte, punendo allo stesso modo, fattispecie criminose dotate di gravità differente.

[75] GIUSEPPE CORASANITI*, op.cit.*

In realtà la dottrina aveva iniziato un lungo dibattito sull'essenzialità di introdurre le misure cautelari in materia informatica[76], ciò che viene criticato è l'intervento generalizzato, che rischierebbe di porsi in netto contrasto con l'art 3 della costituzione, nonché la mancanza di senso logico delle misure adottate, che a parere della dottrina maggioritaria dovrebbero essere destinate ad acquisire la prova mediante procedure mirate certe e verificabili sul piano tecnologico.

Per quanto riguarda la destinazione dei beni informatici o telematici sequestrati o confiscati in quanto utilizzati per la commissione di reati informatici, la norma prevede che: *"I beni e gli strumenti informatici o telematici oggetto di sequestro che, a seguito di analisi tecnica forense, risultino essere stati in tutto o in parte utilizzati per la commissione dei reati di cui agli articoli 473, 474, 615-ter, 615-*quater*, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 635-quinquies, 640-ter e 640-quinquies del codice penale sono affidati dall'autorità giudiziaria in custodia giudiziale con facoltà d'uso, salvo che vi ostino esigenze processuali, agli organi di polizia che ne facciano richiesta per l'impiego in attività di contrasto ai crimini informatici, ovvero ad altri organi dello Stato per finalità di*

[76] A titolo di esempio: Molinari F.M., *Questioni in tema di perquisizione e sequestro di materiale informatico*, in Cass. pen., 2012, pag. 696; *Lorenzetto E., Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenitore al contenuto passando per la copia,* in Cass. pen., 2010, pag. 1522; *Logli A., Sequestro probatorio di un personal computer. Misure ad explorandum e tutela della corrispondenza elettronica*, in Cass. pen., 2008, pag. 2946; *Gabrielli C., Quando il sequestro probatorio ha per oggetto l'hard-disk del computer di un giornalista*, in Giur. it., 2008, pag. 731; *Novario F., Criminalità informatica e sequestro probatorio: le modifiche introdotte dalla L. 18 marzo 2008, n. 48 al codice di procedura penale*, in Riv. dir. proc., 2008, pag. 1069; *CheloMarchia A., Sequestro probatorio di computers: un provvedimento superato dalla tecnologia?*, in Cass. pen., 2005, pag. 1631.

giustizia"; con tale inciso normativo la dottrina si trova in netto contrasto, in quanto ravvisa la sola finalità, visti i limitati investimenti istituzionali, di dotare le forze di polizia e la magistratura di adeguati strumenti tecnologici per contrastare la criminalità informatica.

3.4 PROFILI PROBLEMATICI DELLA NUOVA DISCIPLINA.

La dottrina si trova a dover emettere numerose critiche riguardo la nuova disciplina entrata in vigore con la legge n. 12 del 25 febbraio 2012, in primis evidenzia il controverso raccordo tra la confisca obbligatoria e "forensic", con la quale si intende la mera analisi del disco e delle memorie, al fine di documentare in modo tecnologicamente adeguato, in coerenza con gli obblighi assunti anche a livello internazionale, gli illeciti e interventi penalmente rilevanti su dati o sistemi.

Il legislatore, afferma la dottrina, si limita ad un riferimento sintetico, che sembra sottintendere che prima di tutto vada fatta un'analisi forense sugli oggetti sequestrati, una volta espletata tale analisi, potranno essere assegnati in attesa della conclusione del procedimento, a tal proposito ci si chiede, dopo l'assegnazione, cosa avvenga in caso di archiviazione o assoluzione.

«Non *è una questione secondaria, poiché potrebbe ben immaginarsi una intervenuta sottrazione di ingenti risorse informatiche delle quali solo minima parte sia destinata alla commissione del reato, si immagini il caso di una azienda con più dipendenti, uno dei quali impegnato a commettere reati, e si immagini il caso in cui, magari per una*

sostituzione di credenziali identificative, il reato sia inizialmente attribuito ad altro dipendente invece estraneo ai fatti.

Ed, ancora, si immagini l'uso della stessa risorsa informatica, in modo condiviso tra più utenti, ciascuno dei quali abbia accesso al sistema con differenti livelli di abilitazione e di potenzialità di utilizzazione (peraltro proprio questo è lo schema maggiormente utilizzato dai criminali informatici più scaltri, capaci di cancellare qualsiasi traccia di intervento operativo in grado di ricostruirne le responsabilità effettive, che spesso sono ricondotte apparentemente proprio ad altri soggetti)»[77]

Viene inoltre criticato, come venga sottovalutata la normativa a tutela dei dati personali, con riferimento ai dati contenuti negli apparati in sequestro, ravvisando profili di incostituzionalità, qualora gli "oggetti" sequestrati non siano ricollegabili al reato commesso in via di accertamento.

Dopo aver effettuato un appurata analisi, riguardo alla posizione dottrinaria sulla sopracitata novella legislativa, l'opinione prevalente è la seguente: «Quando *una disciplina nuova pone più problemi di quanti pretenda di risolverne, tanto più in materia penale, sorge il dubbio non solo sulla sua effettiva utilità, ma sulle effettive ragioni di un eccesso legislativo che appare tanto retorico quanto pletorico.*

Si tratta, in altre parole, di un intervento solo apparentemente innovativo, ma in realtà del tutto controproducente rispetto alle intenzioni manifestate dal legislatore, del tutto privo di riscontri in

[77] GIUSEPPE CORASANTI*, op. cit.*

termini di analisi economica costi-benefici (tenendo conto dei costi di ogni sequestro, tanto più dovendosi procedere anche nei casi più semplici ad operazione di analisi prima dell'affidamento dei beni, oltre che delle ingentissime spese di custodia destinate a moltiplicarsi inutilmente) a valere di un limitato effetto ausiliario per uffici inquirenti e di polizia giudiziaria, trattandosi di apparecchiature destinate a rapidissima obsolescenza, e comunque non essendo affatto
la confisca esclusa nella previgente disciplina.»

CONCLUSIONI

Volendo tracciare le linee guida dell'intera riflessione sin qui svolta, riguardo i complessivi e problematici temi trattati, agevoli risultano talune brevi conclusioni finali.

Pur riconoscendo lo sforzo del legislatore nel cercare di creare un sistema legislativo volto a tutelare i beni giuridici messi a repentaglio dal progresso tecnologico ed informatico, è indubbio affermare come il sistema risulti ancora incompleto e poco chiaro, volto a sottolineare una scarsa conoscenza dei fenomeni informatici e tecnologici.

Le norme fino ad ora esaminare rappresentano solo un piccolo passo, verso una tutela siffatta e completa.

Le fattispecie incriminatrici cosi' elaborate, risultano abbastanza obsolete, quasi a sottolineare una difficolta del legislatore di tenere il passo all'incalzante velocità, con i quali tali fenomeni nascono e si diffondono a macchia d'olio.

Il panorama dei reati informatici in Italia vede un numero significativo di previsioni normative volte a sanzionare le condotte di carattere prodromico rispetto alla reale lesione dei beni giuridici.

Il ricorso ad un assetto normativo cosi' fatto, andrebbe accuratamente ponderato, tenendo in considerazione il principio di necessaria offensività, nonché, il disvalore sociale delle condotte tipizzate.

Si potrebbe a tal proposito inserire una riflessione, riguardante l'utilizzo dello strumento penale, in particolare per tutte quelle figure di reato

“anticipatorie” di cui sopra, è davvero necessario prevedere sempre questo complesso di fattispecie penali, che contribuiscono all’ipertrofia dei reati nel nostro ordinamento o, forse sarebbe possibile pensare ad una limitata depenalizzazione, avvalendosi dello strumento amministrativo?.

De iure condendo, il legislatore nel prevedere le fattispecie incriminatrici, dovrebbe avere una piena conoscenza dei fenomeni informatici, anche avvalendosi di appositi supporti in tal senso, non è possibile, in qualsiasi ramo del diritto, trattare una materia senza avere effettivamente la padronanza del fenomeno, soltanto in questo modo è possibile operare delle scelte legislative, ponderate ed efficaci.

BIBLIOGRAFIA E SITOGRAFIA

Maurizio Fumo, *La condotta nei reati informatici, Archivio Penale, settembre–dicembre 2013 fascicolo 3 anno LXV*

L.PICOTTI, *La tutela penale della persona e nuove tecnologie dell'informazione, Cedam, 2013 p.55*

***C.SANTORIELLO E AA.VV**., I reati informatici*

ANTOLISEI, *diritto penale, parte speciale*, vol. I, Milano, 2002, parla di "trasfigurazione del vero". Sul punto, **V. ANGELOTTI**, *Delitti contro il patrimonio*, *Trattato del Florian*, 1936, 391, 414; **DE MARSICO**, *Delitti contro il patrimonio,* 1951; **MANZINI**, *Trattato di diritto penale italiano,* Vol V, Torino, 1952.

***S. BATTAGLIA,** Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio, Altalex 18 settembre 2013*

***M. GROTTO**, La frode del certificatore informatico.*

***ENRICA OBERTO**, I profili distintivi dei reati di frode informatica e di indebita utilizzazione delle carte di pagamento, www.iusinitinere.it*

MAXIME MANZARI,** I reati informatici in particolare: il falso informatico, **maximemanzari.com

***I.SALVADORI**, Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante, rivista di dir. e proc. Penale*

***AVV. FRANCESCO ALBANESE E AVV. VALENTINA PRIVITERA**, La criminalità informatica in Italia*

***C.PECORELLA**, il diritto penale dell'informatica*

***G. ARONICA**, l'indice penale 2010*

*Commentario della Costituzione, Principi fondamentali (artt. 1-12), a cura di **G. Branca**, Zanichelli, Bologna*

***G. SILVESTRI,** L'individuazione dei diritti della persona, in www.penalecontemporaneo.it, 29 ottobre 2018*

***L. PICOTTI**, Diritto penale e tecnologie informatiche: una visione d'insieme, in Trattato di Diritto penale – Cybercrime*

***C. DOMENICALI,** Tutela della persona negli spazi virtuali: la strada del "domicilio informatico", in www.federalismi.it, 28 marzo 2018.*

***V. MILITELLO**, Nuove esigenze di tutela penale e trattamento elettronico delle informazioni, in Riv. trim. dir. pen. eco., 1992*

***L. PICOTTI**, Reati informatici, in Enc. Giur., Agg., 2000*

***F. TAVASSI LA GRECA**, Hacking e criminalità informatica, http://www.altrodiritto.unifi.it*

***L. MONACO**, in Crespi, Stella, Zuccalà (a cura di), Commentario breve al Codice penale, I ed., 1992*

***ANTOLISEI**, Manuale di diritto penale parte speciale*

***LUCA PISTORELLI**, novità legislative – l. febbraio 2012, n., recante "Norme in materia di misure per il contrasto ai fenomeni di criminalità informatica" – Disposizioni rilevanti per il settore penale.*

***GIUSEPPE CORASANITI**, Brevi note in tema di confisca obbligatoria di "beni e strumenti" di commissione dei reati informatici alla luce della legge 15 febbraio 2012, n. 12*

MARINI, *Reati contro la persona*

*Council of Europe action against Cybercrime, **www.coe.int***

ROSITA RIJTANO**, Attacco DDoS (Distributed Denial of Service): Cos'è, come fare, come difendersi. **www.cybersecurity360.it

Frode informatica nelle firme digitali, ***www.studiocataldi.it***

www.101professionisti.it

Avvocatopenletorino.it

www.commissariatodips.it

www.antiphishing.it/