ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Scuola di Scienze
Corso di Laurea in Ingegneria e Scienze Informatiche

I REATI INFORMATICI
ANALISI CRITICA DI ALCUNE FATTISPECIE
ED ESAME DI RELATIVI CASI GIURIDICI

Relazione finale in
INFORMATICA E DIRITTO

Relatore
Prof. CLAUDIA CEVENINI

Presentata da
LAURA CONTI

Seconda Sessione di Laurea
Anno Accademico 2014 – 2015

PAROLE CHIAVE

Codice Penale

Accesso Abusivo

Frode Informatica

Danneggiamento di dati

Legge 23 dicembre 1993 n. 547

"Computers are incredibly fast, accurate, and stupid.
Human beings are incredibly slow, inaccurate, and brilliant.
Together they are powerful beyond imagination."
ALBERT EINSTEIN

Indice

Introduzione

Lo sviluppo tecnologico e la nascita di Internet, in particolare del World Wide Web, ha portato alla costituzione di un nuovo canale di comunicazione, il quale è tutt'ora considerato come la rivoluzione del secolo. La rete non rappresenta solo la possibilità di spedire o ricevere informazioni tra persone che si trovano in diverse parti del mondo ma, insieme all'utilizzo dei sistemi informatici, costituisce un veicolo per la realizzazione di illeciti. Lo scopo di questa tesi di laurea è di presentare e analizzare in modo critico i principali reati informatici.

La scelta di questo argomento, forse considerato atipico per quanto riguarda il corso di laurea, è stata eseguita con l'obiettivo di soffermarsi sull'altro aspetto dell'informatica. Di quest'ultima si nota principalmente la sembianza della comodità nella vita di tutti i giorni, dello sviluppo, degli innumerevoli vantaggi che questo comporta per la società. L'apparenza inganna, o meglio, nasconde sempre una prospettiva negativa. Molti non sono a conoscenza degli innumerevoli crimini che, con il tempo, si sono venuti a delineare e che la dottrina ha inizialmente accostato alle fattispecie "materiali". Un esempio è il reato di accesso abusivo ad un sistema informatico assimilato al reato di violazione di domicilio. Si ritiene sia di fondamentale importanza porre l'attenzione e venire a conoscenza di questi reati, non solo a scopo didattico, ma anche e soprattutto per saperli riconoscere nella quotidianità e potersi tutelare nel miglior modo possibile.

Il punto di forza della tesi è quello di non fornire un'asettica descrizione dei reati in sé, ma svolgerne un'analisi accurata e, inoltre, esaminare casi reali per ciascuno di essi. In questo modo è possibile concretizzare la fattispecie teorica, effettuando una ricerca all'interno delle banche dati contenenti sentenze. Non si tratta di una semplice ricerca, in quanto è necessario inizialmente fare una scrematura dei casi per ciascun reato e, successivamente, analizzare le diverse sentenze scelte per determinare quale sia la migliore per un'analisi il più possibile completa. Lo studio della sentenza è consistito in diverse riletture

della stessa, per capire in primo luogo se fosse pertinente allo scopo e, nelle successive letture, per scegliere quali parti fossero di interesse e quali non dovessero essere prese in esame. L'ultima fase è relativa ad una rielaborazione e riflessione di quanto scelto.

Non tutte le fattispecie di reato informatico saranno prese in esame. Non saranno trattati ad esempio il cyber-bullismo, il cyber-stalking, la pornografia infantile e pedofilia online. Nel primo capitolo ne sarà dato un breve accenno.

Le ricerche sono state effettuate attraverso diverse banche dati. Principalmente è stata usata la banca dati "DeJure", in cui sono stati cercati i testi degli articoli e le sentenze per i vari reati. Oggetto di consulto sono anche state le banche dati "Dottrina e Dottrine" e "Biblioteca WKI". Si è fatto riferimento ad articoli presi da siti giuridici, per i quali si è verificato costituissero una fonte sicura. Sono state inoltre letti diversi libri in materia di reati informatici, da cui si è preso spunto.

La tesi espone al primo capitolo una panoramica storica e generale sui reati informatici, ponendo l'accento sulle date di fondamentale importanza per la materia. È inoltre fornito un profilo del soggetto agente dei crimini informatici.

Successivamente, nel secondo capitolo, è mostrata in modo più approfondito la Legge 23 dicembre 1993 n. 547, elencando inoltre i reati presenti nel Codice Penale italiano, i quali saranno studiati in seguito. È anche fornita un'analisi della legge di ratifica della Convenzione europea di Budapest.

Il terzo capitolo è suddiviso in diverse sezioni, ciascuna delle quali analizza i reati elencati in precedenza. Ogni sezione è articolata in una sottosezione in cui sono esaminati uno o più casi di interesse. Si tratta del capitolo cardine della trattazione.

Infine, il quarto ed ultimo capitolo, esamina l'esigenza di avere una normativa comune tra i vari stati del mondo. I reati informatici hanno infatti la caratteristica di a-territorialità, che rende necessaria una cooperazione internazionale. È anche delineata un'analisi della situazione relativa agli Stati Uniti d'America.

Capitolo 1

I Reati Informatici

In questo capitolo si definisce una panoramica generale sui reati informatici, mettendone in evidenza il percorso storico. Si mostra inoltre l'evoluzione del profilo dei criminali informatici.

1.1 Diffusione dei reati informatici

L'utilizzo sempre più diffuso del computer ha generato la diffusione di comportamenti illeciti, i quali sono convenzionalmente ricondotti alla dizione di reati informatici o computer crimes. Si tratta di una disciplina piuttosto recente che può essere considerata come il risvolto negativo dello sviluppo tecnologico dell'informatica e della telematica. Tale sviluppo ha delineato nuovi scenari negli ultimi decenni. Infatti, in un periodo di tempo piuttosto breve, la gran parte delle attività umane che erano svolte manualmente o per mezzo di apparecchiature meccaniche, sono state sostituite da implementazioni digitali di gran lunga più efficienti. Un esempio evidente è costituito da database informatici centralizzati che hanno permesso la sostituzione degli enormi archivi documentali i quali, non molto tempo fa, creavano grandi problemi di gestione. Un'altra caratteristica delle tecnologie digitali è la netta separazione dell'informazione dal supporto, con una conseguente facilità di riproduzione e trasferimento del contenuto, indipendentemente dal supporto su cui esso è memorizzato. La facilità di diffusione del dato digitale è ulteriormente favorita dallo sviluppo delle reti telematiche, in particolare la rete Internet. Come già evidenziato in precedenza, tutto ciò offre grandi possibilità di crescita per la società. Si sviluppano infatti attività quali l'e-commerce e l'home-banking, che se da una parte rendono più agevole la vita quotidiana, dall'altra la legano strettamente alla rete. Se pertanto la maggior parte degli interessi si basano sulla tecnologia informatica, di conseguenza anche le attività illecite ne seguono l'evoluzione. Alcune fattispecie di reato tradizionale, come furti

di informazioni, frodi, spionaggio, pedofilia e terrorismo, sono in grado ora di articolarsi prevalentemente all'interno dei nuovi sistemi digitali. Si parla di hacking, diffusione di virus informatici, frodi telematiche, spamming, diffusione di informazioni illegali online, ma anche ad esempio di cyber-pedofilia e cyber-terrorismo. Questi ultimi due aspetti non saranno trattati dalla tesi in esame, ma si riteneva necessario un loro accenno. Risulta necessario quindi, sviluppare misure idonee a contrastare il progredire di questi crimini. Da una parte è possibile prevenire tali reati responsabilizzando l'utenza sulle potenzialità, ma anche sui rischi, derivanti dall'utilizzo dei sistemi informatici. Dall'altra parte sono adottate delle misure di repressione dei reati informatici, che possiamo trovare nel Codice Penale e nelle disposizioni comunitarie. Nel terzo capitolo, oltre all'analisi dei singoli reati, saranno proposte le possibilità preventive di cui l'utenza può usufruire per scongiurare, nel miglior modo possibile, crimini informatici a proprio danno.

Tuttavia non è stata ancora fornita una definizione di ciò che è un reato informatico. In questa tipologia di crimini vengono fatti rientrare gli illeciti in cui l'elaboratore ha un ruolo di strumento attivo, risultando essere l'oggetto o il mezzo per la commissione del reato. L'utilizzo di un sistema di elaborazione è quindi necessario, poiché l'illecito deve essere rivolto ad un computer o presupporre l'utilizzo di un sistema informatico. In base ad una definizione più adeguata alla scienza penalistica, sono computer crimes "ogni tipo di violazione penale commessa per mezzo o con l'ausilio di un sistema o programma informatico e/o avente ad oggetto lo stesso sistema o programma informatico". Per sistema informatico o telematico si intende "qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati". Per programma informatico si intende invece "una sequenza di istruzioni ordinate mediante algoritmi, impartita al computer attraverso il quale il programma stesso opera". Le definizioni sopra citate sono prese dall'art. 1 della Convenzione di Budapest emanata dal Consiglio d'Europa nel 2001.

1.2 Cenni storici

La diffusione degli strumenti informatici ha comportato rilevantissime trasformazioni sociali, non soltanto in senso positivo. Il mondo criminale ha ben presto intuito la possibilità di avvalersi del mezzo informatico a fini illeciti. Il termine hacker nasce con l'informatica ed è rivolto a identificare quegli individui che non hanno l'obiettivo criminoso, ma attaccano gli strumenti informatici

con il solo scopo di capirli e smontarli, senza arrecare danno o sottrarre informazioni. Il termine deriva dal verbo inglese "to hack" che tradotto significa "scomporre, fare a pezzi". Lo scopo che si propone un hacker è quello di provare ad accedere ad un sistema informatico protetto, al fine di capirne il funzionamento, studiarlo, ma non danneggiarlo. Questi soggetti sono persone per le quali la programmazione informatica costituisce una passione, e hanno l'obiettivo principale di analizzare come i sistemi sono costruiti e come funzionano, per scoprirne le debolezze o per innovare ed implementare le applicazioni. Dal punto di vista storico il primo riferimento alla pirateria informatica è avvenuto alla fine degli anni cinquanta al M.I.T (Massachusetts Institute of Technology), dove iniziava a diffondersi la "cultura-hacker", soprattutto tra docenti e studenti interessati agli studi sugli elaboratori elettronici. A quell'epoca la sperimentazione rappresentava la tecnica di lavoro sui sistemi informatici, i quali potevano essere violati per elevare il livello delle conoscenze scientifiche e verificare l'efficacia delle protezioni contro le intrusioni, anche se non era consentito danneggiare i programmi e le informazioni. Nel tempo le tecniche di "hacking" sono state usate a scopo criminoso, introducendo anche il nuovo termine "cracker", che deriva dal verbo "to crack" col significato di "distruggere". È facile comprendere la sostanziale differenza tra "hacker" e "cracker", anche se, dal punto di vista legislativo, l'accesso abusivo ad un sistema informatico senza lo scopo di danneggiamento è considerato ugualmente reato. "Hacker" rimane l'espressione, impiegata in modo universale, per indicare ogni tipo di comportamento che integra i reati commessi con il ricorso a strumenti informatici. Rispetto al passato, l'analisi del profilo di un soggetto che commette reati informatici è cambiata. La sottile separazione tra mondo fisico e virtuale ha dei risvolti psicologici significativi, per cui chi compie un reato informatico non percepisce il disvalore criminale della propria condotta e non si identifica come, ad esempio, un rapinatore di strada. Il profilo soggettivo di un cyber criminale è costituito da un'istruzione medio-alta, assenza di comportamento violento e antisociale, ridotta percezione del crimine e buona capacità di premeditazione e organizzazione[1].

Dopo aver spiegato come l'attività criminosa nei confronti dei sistemi informatici si sia diffusa e quali soggetti siano i portatori di questa problematica, si definisce a questo punto il percorso italiano per quanto riguarda la normativa contro l'emergente fenomeno dei crimini informatici. La legislazione italiana ha approvato la Legge 23 dicembre 1993 n. 547, identificata come "Modificazioni ed integrazioni alle norme del Codice Penale e del codice di procedura penale in tema di criminalità informatica". Tale legge è entrata poi in vigore il

[1]Battaglia Salvatore, *Criminalità informatica al tempo di Internet: rapporti tra phishing e riciclaggio*, http://www.altalex.com/, 2014

14 gennaio 1994. Nel periodo che ha preceduto l'approvazione della L. 547/93, la dottrina e la giurisprudenza tentarono di ricondurre i reati informatici a fattispecie tradizionali. Il problema non si poneva in relazione alla parte fisica dell'elaboratore, l'hardware, che può essere riconosciuto nelle classi di danneggiamento e furto, quanto per i crimini commessi attraverso l'elaboratore che coinvolgono il software e i dati contenuti nel sistema stesso. Prima degli anni '90 si possono citare due provvedimenti con l'obiettivo di reprimere i reati informatici, costituiti dalla Legge 18 maggio 1978 n. 191, che introduceva nel Codice Penale l'art. 420 contro l'attentato ad impianti di elaborazione dati, e dalla Legge 1 aprile 1981 n. 121, che definisce la prima forma di tutela dei dati archiviati in un sistema informatico. Da considerare anche il Decreto Legislativo 29 dicembre 1992 n. 518, in attuazione della Direttiva 91/250/CEE del Consiglio del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore. Di fondamentale importanza è la Convenzione di Budapest sul cybercrime del 2001, che ha imposto agli stati membri dell'Unione Europea l'adozione di misure per la repressione penale dei crimini informatici. La legislazione italiana ha ratificato la Convenzione con la Legge 18 marzo 2008 n. 48, entrata in vigore l'8 novembre 2008. In ultimo, la Legge 15 febbraio 2012 n. 12, prevede un'importante modifica dell'art. 240 c.p., introducendo la confisca degli strumenti informatici che risultino essere stati usati, in tutto o in parte, per la commissione dei reati previsti dalla L. 547/93 e dalla L. 48/2008.

Capitolo 2

La legislazione italiana

In questo capitolo è trattata in modo più dettagliato la Legge 23 dicembre 1993 n. 547, stilando un elenco dei reati informatici che saranno oggetto di analisi. Si esamina inoltre la legge di ratifica della Convenzione di Budapest.

2.1 Dettaglio della Legge 23 dicembre 1993 n. 547

Il primo intervento del legislatore italiano allo scopo di contrastare la criminalità informatica risale al 1993, anno in cui è stata emanata la L. 547/93. Si trattava di un provvedimento necessario poiché, fino a quel momento, alle condotte realizzate ai danni dei sistemi informatici, si applicavano le fattispecie delittuose già presenti nel Codice Penale. Il comportamento adottato aveva una dubbia fattibilità, in quanto violava sia il principio di legalità, che quello di tassatività del diritto penale. Il primo "vieta di punire qualunque fatto che non sia espressamente previsto dalla legge" sulla base dell'art. 1 del Codice Penale, il secondo esprime il divieto per il giudice e per il legislatore di estendere la disciplina contenuta nelle norme incriminatrici oltre i casi in esse espressamente previsti. Quest'ultimo è pertanto rivolto ad evitare arbitrarie ingerenze nelle norme penali da parte del potere giudiziario[1]. Le norme a disposizione rendevano quindi prive di sanzione le condotte relative al cybercrime.

I reati introdotti sono i seguenti:

- art. 615-ter c.p. "Accesso abusivo a un sistema informatico o telematico",

[1] Cristina Cosentini, *Il principio di legalità in materia penale*, http://www.altalex.com/, 2010

- art. 615-quater c.p. "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici",
- art. 615-quinquies c.p. "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico",
- art. 617-quater c.p. "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche",
- art. 617-quinquies c.p. "Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche",
- art. 617-sexies c.p. "Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche",
- art. 635-bis c.p. "Danneggiamento di informazioni, dati e programmi informatici",
- art. 640-ter c.p. "Frode informatica".

La legge ha inoltre modificato i seguenti articoli del Codice Penale:

- art. 392 c.p. "Esercizio arbitrario delle proprie azioni",
- art. 616 c.p. "Violazione, sottrazione e soppressione di corrispondenza",
- art. 621 c.p. "Rivelazione del contenuto di documenti segreti".

Inoltre, sono state estese:

- le ipotesi di falsità di cui al Capo III (Della falsità in atti) del Titolo VII (Dei delitti contro la fede pubblica) ai documenti informatici,
- art. 420 c.p. "Attentato a impianti di pubblica utilità".

Il legislatore italiano ha poi ratificato la Convenzione di Budapest soltanto nel 2008, con una legge che, oltre ad intervenire in forte ritardo, introduce significative modifiche alle disposizioni penali in tema di reati informatici. Per quanto riguarda la riforma di fattispecie criminose, si hanno modifiche dei seguenti articoli:

- art. 491-bis c.p., relativo al falso informatico,
- art. 495-bis c.p., relativo alla falsa dichiarazione o attestazione al certificatore di firma elettronica,

- art. 615-quinquies c.p., relativo alla diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico,
- artt. 635-bis, 635-ter, 635-quater, 635-quinquies c.p., relativi al danneggiamento informatico,
- art. 640-quinquies c.p., relativo alla frode informatica del certificatore.

Risultano abrogati i commi 2 e 3 dell'art. 420 c.p. relativi all'attentato nei confronti di impianti di pubblica utilità, poiché tali disposizioni sono state inserite all'art. 635-quinquies c.p..

La legge di ratifica, 18 marzo 2008 n.48, non ha creato un settore specifico del diritto penale riservato alla criminalità informatica, ma ha dislocato i vari articoli sulla base dell'oggetto giuridico sottoposto a tutela. I "reati informatici" del Codice Penale sono stati quindi inseriti all'interno di titoli e capi preesistenti, designati alla protezione di beni giuridici già identificati. La scelta del legislatore risulta condivisibile, in quanto non è possibile individuare un unico bene giuridico alla cui tutela siano sottoposte tutte le fattispecie criminose considerate dalla Convenzione di Budapest. La ratifica alla Convenzione ha inoltre completato il sistema sanzionatorio, prevedendo un'ipotesi di responsabilità amministrativa a carico dell'ente nel cui interesse sia stato commesso un crimine informatico. È ovviamente necessaria la presenza di un vantaggio per l'ente, il quale non potrà rispondere nel caso in cui il suo dipendente abbia commesso il reato nell'interesse esclusivo proprio o di terzi.

Capitolo 3

Spiegazione e analisi dei reati

In questo capitolo sono trattati i reati di cui al capitolo secondo. Inoltre, per ciascuno di essi, è esaminato almeno un caso giuridico.

3.1 Accesso abusivo ad un sistema informatico

Art. 615-ter - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

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 di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di 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'art 615-ter del Codice Penale è inserito nel Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio". Il bene giuridico oggetto della norma è il "domicilio informatico", inteso come estensione del domicilio fisico e spazio virtuale facente parte della sfera personale di un individuo che, come tale, deve essere tutelato. La differenza del domicilio informatico da quello fisico, risiede nella sua caratteristica di spazio flessibile e aperto, il quale non può essere tutelato a priori ma può esserlo, in base alla volontà del titolare di renderlo riservato. Poiché tale reato sussista, è necessaria l'evidente volontà dell'individuo di escludere terzi soggetti dall'accesso al sistema. Tale disposizione si afferra immediatamente nell'articolo, da cui un sistema, per poter subire accesso abusivo, deve essere protetto da una qualsiasi forma di sicurezza. Queste ultime possono essere costituite sia da forme di protezione logica che fisica, come indicato da una sentenza della Cassazione Penale (Cass. Pen., sez. V, 7-11-2000, n. 12732, CP, 2002, 1015). Esempi di protezione logica di un sistema informatico sono l'impostazione di un account (con nome utente e password) o l'adozione di un firewall per il controllo degli accessi. La protezione fisica può essere invece predisposta con meccanismi di custodia degli impianti, quali la presenza di un vigilante o di una porta blindata. Misure di sicurezza più all'avanguardia possono essere costituite da sistemi biometrici. La norma prevede due condotte, entrambe penalmente rilevanti:

- il mero accesso al sistema protetto da misure di sicurezza,
- il mantenimento all'interno dello stesso contro la volontà espressa o tacita del titolare.

In base a quanto indicato dalla norma, l'ingresso deve essere "abusivo", pertanto è necessario accertare che l'accesso sia effettivamente illecito e che non sia consentito da norme di diritto civile o amministrativo. Nel caso esistessero delle giustificazioni il reato decadrebbe. Da prendere in considerazione è il caso in cui l'ingresso sia lecito, ma il trattenimento nel sistema avvenga con finalità diverse da quelle effettivamente autorizzate. Si tratta del caso in cui dipendenti o pubblici ufficiali utilizzino la loro figura per scopi diversi da quelli consentiti. Sono sanzionabili, dunque, anche le intrusioni che si realizzino con una permanenza illecita successiva ad un ingresso legittimo. Leggermente diverso il caso in cui un operatore acceda a sezioni del sistema a lui interdette. Se tali diverse sezioni non sono protette da misure di sicurezza il reato non sussiste, ma tornerebbe ad essere rilevante come illecito, se l'accesso avvenisse per finalità non consentite.

Di grande importanza è l'aggravante che riguarda la figura di operatore del sistema. Quest'ultima si identifica in quei soggetti che, a causa delle loro

funzioni, si trovano in una posizione di vantaggio nell'utilizzo, anche improprio, del sistema informatico. L'aggravio della pena si giustifica nel punire in modo più severo il comportamento illecito più facile da commettere. L'operatore di un sistema non è soltanto il tecnico programmatore, analista, sistemista, ma può trattarsi di qualsiasi soggetto che interviene, o può intervenire facilmente, sul sistema grazie alle proprie mansioni.

Da puntualizzare il fatto che l'art. 615-ter non fa riferimento a possibili danni causati dall'accesso abusivo al sistema, ma ha lo scopo di reprimere esclusivamente l'atto di accesso. Può però essere realizzato in concorso con il reato di danneggiamento informatico, nel caso in cui le due condotte si realizzino in tempi non contestuali. Ciò si verifica quando il soggetto accede al sistema e, solo in un secondo momento, inizia a danneggiarlo. Se invece l'accesso viene realizzato contestualmente e al solo fine di condotta vandalica, si parla di una fattispecie di reato unica prevista all'art. 635-bis c.p..

3.1.1 Caso giuridico

Di seguito è analizzata una sentenza riguardo l'accesso abusivo ad un sistema informatico.

- Tribunale sez. II Firenze
- 30/01/2014
- Numero 657

Il soggetto è inizialmente imputato di violazione del sistema informatico di amministrazione e gestione dell'home banking, relativo alla Cassa di Risparmio di Firenze. L'imputato si è abusivamente introdotto nello spazio attribuito in esclusiva ad una cooperativa, usando i codici bancari associati al legale rappresentante di quest'ultima e sostituendosi indebitamente alla sua persona. Attraverso l'utilizzo di tali codici, nel giorno 6 ottobre 2010, il soggetto si è disposto dal dominio dell'ente sopra indicato, un bonifico di euro 2739 sul proprio conto.

Il Pubblico Ministero ha proposto una condanna ad anni uno e mesi tre di reclusione.

Il dibattito tra le parti ha accertato, senza alcun dubbio, la responsabilità penale dell'imputato per l'accesso abusivo al sistema e la tentata frode informatica. Per quanto riguarda la sostituzione di persona, vi è stata invece una pronuncia assolutoria per la non sussistenza del fatto. Vengono esaminate ora le motivazioni che hanno portato a tale conclusione.

Dalla documentazione acquisita durante il processo, si ha prova che la sera del 6 ottobre 2010, dal conto corrente online della cooperativa è stato realmente

disposto un bonifico di 2739 euro a favore dell'imputato. Una dipendente della cooperativa ha inoltre testimoniato di non avere eseguito tale bonifico, sostenendo inoltre che quella sera a quell'ora nessuno era presente in ufficio. Per di più, successivamente, il computer è stato portato in riparazione, poiché rimaneva acceso nonostante il comando di spegnimento. La ditta di manutenzione ha effettivamente trovato la presenza di alcuni virus. In base a queste vicende, il giudice ha riconosciuto il reato di accesso abusivo a sistema informatico senza le aggravanti di danneggiamento né del sistema di home banking, né dei dati o programmi in esso contenuti. È inoltre stato riconosciuto un tentativo di frode informatica, che non si è concretizzata in quanto il bonifico è stato bloccato dal Servizio Antifrodi dell'istituto di credito. Non è stata riconosciuta la fattispecie di sostituzione di persona che era stata contestata all'imputato. Quest'ultimo non ha mai falsamente assunto l'identità del responsabile legale o indotto altri in errore, ma ha usato soltanto i codici di accesso, a proprio esclusivo profitto personale.

Si determina piena responsabilità dell'imputato, al quale si infligge un anno di reclusione (suddiviso in 8 mesi per accesso abusivo e 4 mesi per tentata frode) più il pagamento delle spese processuali.

3.2 Detenzione e diffusione abusiva di codici di accesso

Art. 615-quater - Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzione idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

L'art. 615-quater del Codice Penale si trova al Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro l'inviolabilità del domicilio", così come l'art. 615-ter. Inoltre, come quest'ultimo, configura una situazione di pericolo che anticipa un evento dannoso. La tutela non è più riferita al domicilio informatico, ma al possesso esclusivo dei codici di accesso ad esso. Tali codici devono essere protetti da misure di sicurezza e possono essere costituiti da: strumenti virtuali (password e codici), strumenti materiali (smart card e chiavi meccaniche), strumenti biometrici (impronte e sistema vocale). Il reato si configura attraverso diverse fattispecie, ma comunque a prescindere dall'utilizzo dei codici posseduti illecitamente. All'interno dell'articolo sono puniti i seguenti comportamenti:

- il "procurarsi" i codici da soggetti che li possiedono,
- la "riproduzione" del codice, nel caso in cui l'agente riesca a crearlo in modo autonomo,
- la "diffusione" dei codici nel caso di comunicazione a soggetti indeterminati,
- la "comunicazione" dei codici a soggetti determinati,
- la "consegna" nel caso in cui si abbiano codici di tipo fisico.

La norma punisce anche chi permette ad altri la possibilità di eseguire i comportamenti sopra elencati, attraverso l'indicazione di istruzioni tecniche su come ottenere i codici. Tuttavia, il reato non sussiste se tali condotte non provocano un profitto personale o nei confronti di altri, o se comunque non provocano un danno a terzi.

Sono anche previste delle aggravanti di pena in due diverse situazioni. Il primo aggravio riguarda la detenzione o diffusione di codici relativi a sistemi informatici o telematici appartenenti allo Stato o altro ente pubblico. La maggiore pena è giustificata dall'importanza di tali sistemi su scala pubblica. Il secondo aggravio riguarda l'esecuzione del reato da parte di operatori del sistema. In questo caso, come avveniva anche per l'art. 615-ter, i soggetti si trovano in una posizione di vantaggio, in quanto grazie alla loro funzione, hanno la possibilità di accedere al sistema e commettere il reato senza particolari difficoltà. Il reato si configura anche quando la collaborazione tra l'agente e il titolare del sistema è occasionale.

3.2.1 Caso giuridico

In banca dati non è stata rinvenuta alcuna sentenza per quanto riguarda il reato di "Detenzione e diffusione abusiva di codici di accesso". Tuttavia, è stato trovato un caso in cui uno dei capi di accusa degli imputati può essere ricondotto al reato sopra citato, mentre infine è stato assorbito da una fattispecie diversa. Di seguito è esaminata la motivazione.

- Tribunale di Roma
- 19/10/2010

Il caso si riferisce a due soggetti sorpresi davanti ad uno sportello bancomat, intenti al sospetto atto di prelievo di contanti, mediante l'utilizzo di diverse carte di credito.

Gli imputati sono stati citati per quattro capi di accusa. Sulla base delle prove raccolte, il giudice ha riconosciuto la penale responsabilità degli imputati per il reato di cui all'articolo 12 del d.l. 3 maggio n. 143, convertito dalla legge 5 giugno 1991 n. 197. Questo articolo non è più in vigore, in quanto abrogato dal d.lgs. 21 novembre 2007 n.231, ma è stato sostituito dall'art. 55 comma 9 dello stesso decreto legislativo. Tale reato riguarda la condotta di chi, al fine di trarne profitto, abbia acquisito, possieda e abbia indebitamente utilizzato senza autorizzazione, una carta di credito o altro documento similare di provenienza illecita o comunque alterato. Alla perquisizione dei soggetti, in seguito ad una segnalazione di un passante, sono state rinvenute 17 carte bancomat con banda magnetica e codici impressi con un pennarello, oltre a circa euro 2.000 in contanti. La Polizia postale ha successivamente eseguito degli accertamenti sui supporti sequestrati, confermando che si trattasse di carte clonate. Tali supporti magnetici rientrano nei "documenti analoghi" alle carte di credito o pagamento abilitate al prelievo dei contanti. Gli avvocati difensori hanno cercato di far assolvere gli imputati, sulla base della mancata prova di effettivo

utilizzo delle carte clonate, ma il reato a loro contestato punisce anche solo il possesso di tali supporti. Oltre all'illecita detenzione, sussiste anche la finalità di profitto, provata dal denaro rinvenuto e dalla mancanza di conti intestati ai soggetti stessi.

Le accuse di cui al secondo capo sono quelle relative all'art. 615-quater c.p. di nostro interesse. La detenzione e diffusione abusiva di codici di accesso (PIN) ai sistemi informatici di prelievo, non risulta applicabile al caso in esame. Non è riscontrata la "diffusione" dei codici in possesso degli imputati, i quali li hanno utilizzati al solo scopo di prelievo bancomat. La "detenzione" di tali codici potrebbe essere ricondotta all'art. 615-quater, ma essendo i codici incorporati nei supporti magnetici, tale condotta risulta assorbita nella fattispecie punita al primo capo di accusa.

Per completezza vengono analizzati brevemente anche gli altri due capi di accusa. La fattispecie al terzo capo riguarda l'installazione di apparecchiature al fine di intercettare comunicazioni informatiche. Poiché non sono state rinvenute attrezzature di questo tipo, gli imputati sono stati assolti per questo capo di accusa. Anche la condotta all'ultimo capo, relativa al reato di frode informatica, non sussiste. Infatti quest'ultimo presuppone l'alterazione del funzionamento del sistema informatico o l'intervento senza diritto su dati, informazioni o programmi contenuti nel sistema stesso. Gli imputati non alterano il sistema, ma vi introducono un sopporto che abilita al prelievo secondo il corretto funzionamento del circuito.

Si ritiene importante citare la dichiarazione della Cassazione penale sez. II del 3 ottobre 2013 n. 47021, secondo la quale integra il reato di detenzione abusiva di codici di accesso a servizi informatici (art. 615-quater c.p.) e non quello di ricettazione, la condotta di chi riceve i codici di carte di credito e li inserisce in carte clonate poi utilizzate per il prelievo di denaro contante attraverso il sistema bancomat.

3.3 Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

Art. 615-quinquies – Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

L'art. 615-quinquies del Codice Penale si trova al Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro l'inviolabilità del domicilio". L'articolo completa la normativa preventiva per assicurare il diritto dell'individuo di godere in modo indisturbato del proprio sistema, senza che gli stessi subiscano danni illeciti. La presenza di un articolo del Codice Penale riferito unicamente agli strumenti in grado di danneggiare un sistema informatico, permette di capire quanto questi siano diffusi. Tali congegni possono essere sia hardware, ad esempio smart card o pen drive USB, che specialmente software per quanto riguarda i malware. Quest'ultimo termine deriva da "malicious software", ma è generalmente conosciuto con il termine di virus, anche se impropriamente. Esistono diverse tipologie di malware, tutte accomunate dalla finalità dannosa per il sistema informatico; di seguito ne vengono esaminati brevemente alcuni.

Virus sono software di piccole dimensioni, specializzati per eseguire poche e semplici operazioni, ottimizzati ad usare il minor numero di risorse per rendersi il più possibile "invisibili". Il loro scopo è quello di riprodursi e diffondersi ogni qual volta il file venga aperto. Per poter funzionare necessitano di un programma chiamato software ospite. Il virus altera il programma da infettare, inserendo tra le prime istruzioni un salto alla sua copia ed, alla fine di essa, un salto all'inizio del file. L'utente non è in grado di accorgersi della sua esecuzione, ma attualmente è possibile una protezione efficace dai virus per mezzo di programmi antivirus, se questi ultimi sono costantemente aggiornati.

Trojan Virus rispetto alla categoria precedente non si replicano, ma sono software all'apparenza innocui che svolgono funzioni tutt'altro che utili. Agiscono sui file del sistema infettato, permettendo anche a terzi l'accesso. Il loro

nome deriva dall'espediente di Ulisse del cavallo di Troia, ricordandone infatti il comportamento. È possibile difendersi da essi tramite programmi antivirus.

Worms creano copie di sé stessi su altri sistemi ai quali sono connessi in rete, con un'elevata capacità di propagazione e senza bisogno di un software ospite. Sono generalmente diffusi attraverso messaggi di posta elettronica.

Logic Bombs sono programmi che si attivano a distanza di tempo dal momento in cui sono stati installati.

Spyware sono software che in modo invisibile raccolgono informazioni sull'attività dell'utente. Queste sono poi trasmesse attraverso la rete a delle organizzazioni, le quali ne trarranno profitto tramite l'invio di pubblicità mirata agli utenti.

La norma è stata modificata in modo significativo dall'art. 4 della legge del 2008 di ratifica della Convenzione di Budapest, rendendola più efficace rispetto al testo del 1993. Originariamente le condotte punite erano quelle di diffusione, comunicazione e consegna, mentre attualmente sono configurabili anche le condotte del procurarsi, mettere a disposizione di altri, produrre, riprodurre e importare apparecchiature, dispositivi o programmi dannosi. La Convenzione prevedeva la punibilità rispetto al possesso di una soglia numerica di tali strumenti, ma tale disposizione non è stata raccolta dalla ratifica. Non si esclude però che la quantità possa essere considerata, specie per la dimostrazione del dolo specifico. Le condotte sono infatti punite soltanto se poste in modo specifico al danneggiamento del sistema o dei suoi contenuti.

3.3.1 Caso giuridico

In relazione al reato sopra esposto, è stato scelto di esaminare il caso Vierika.

- Corte appello Bologna sez. II
- 27/03/2008

Il Tribunale di Bologna, con sentenza n. 1823 del 21 luglio 2005, ha giudicato l'imputato in merito agli artt. 615-ter c.p. e 615-quinquies c.p.. L'oggetto della controversia è un malware chiamato "Vierika". Quest'ultimo è un programma, creato dall'imputato, allo scopo di insinuarsi nei sistemi informatici.

La trasmissione è avvenuta con l'invio del malware al provider Tiscali, dal quale si è poi introdotto e diffuso nei sistemi di circa 900 utenti. Al loro interno, "Vierika" acquisiva dati riservati e compiva azioni che alteravano l'ordinario funzionamento dei sistemi. Tale condotta avveniva nel corso dell'anno 2001. Durante la controversia, si è verificato che Vierika è un worm programmato in linguaggio Visual Basic e costituito da due script diversi, che denotano due differenti azioni. Un worm, a differenza di un virus, è una categoria di malware che non necessita di un file eseguibile per diffondersi, ma si auto-replica spedendosi direttamente agli altri computer. Il primo insieme di comandi è inviato come allegato ad una email, la quale ha come oggetto "Vierika is here". L'allegato è costituito dal file infetto "Vierika.jpg.vbs", ma l'ultima estensione non è visibile all'utente che viene così indotto in inganno pensando che si tratti di un semplice file di immagine. Al contrario, scaricando l'allegato il destinatario installa, a sua insaputa, un programma. Quest'ultimo modifica il registro di configurazione del sistema Windows, riconfigurando al minimo le protezioni del browser Internet Explorer ed inserendo come home page predefinita la pagina web con indirizzo http://web.tiscalinet.it/krivojrog/vierika/Vindex.html. Pertanto, all'avvio della navigazione in Internet, l'utente è ricondotto all'indirizzo sopra citato, in cui viene automaticamente scaricata una stringa di comandi. Il secondo script contiene il documento Vindex.html che crea una partizione nel disco rigido dell'utente, dove viene annidata la prima parte del codice virale. Inoltre, sempre all'insaputa dell'utente, il programma produce un comando che invia a tutti gli indirizzi di posta elettronica Outlook una email avente come oggetto l'allegato "Vierika.jpg.vbs". Si è avuta così una diffusione esponenziale del worm ad effetto autoreplicante. Attraverso tracce informatiche nel server del gestore Tiscali, si è identificato l'imputato il quale, registrato presso il provider con il nickname "Krivoj", è l'amministratore del sito all'indirizzo web in precedenza nominato. Durante perquisizione e sequestro, l'imputato ha riconosciuto di essere il creatore di Vierika e ha collaborato mostrando i file di programmazione e masterizzandone lui stesso delle copie, sottoposte poi a sequestro. Il funzionamento del worm è stato riportato in aula dal Nucleo Crimini Informatici della Guardia di Finanza di Milano. Le prove sono state ritenute dal giudice esaustive, negando la perizia informatica richiesta dalla difesa, in quanto la difesa stessa non metteva in dubbio il funzionamento descritto del programma. Questa parte è stata oggetto di discussione poiché, per legittimità, è indicata come necessaria la perizia per l'accertamento tecnico nella fattispecie dei computer's crime. Il Tribunale di Bologna ha ritenuto l'imputato colpevole per entrambi i reati. La responsabilità per il reato all'art. 615-ter c.p. è riscontrabile dal numero degli accessi al sito dell'imputato, pari a 829, che corrispondono ad altrettante abusive introduzioni nei sistemi informatici degli utenti. In primo grado sono state riconosciute le

aggravanti di violenza sulle cose e danneggiamento dei dati, per l'alterazione del funzionamento del browser Explorer. Riguardo all'art. 615-quinquies c.p., la responsabilità dell'imputato è accertata poiché Vierika altera la funzionalità informatica del sistema infettato, modificando i parametri di protezione del browser. La pena inflitta è di sei mesi di reclusione, sostituiti dalla sanzione pecuniaria corrispondente.

I principali motivi per cui la difesa ha impugnato la sentenza sono:

- il vizio della sentenza basata su una ricostruzione priva di perizia,
- l'assenza delle fattispecie aggravanti dell'art. 615-ter c.p.,
- l'assenza di danneggiamento o alterazione di sistema e dati previsti dall'art. 615-quinquies c.p..

Per quanto riguarda il primo punto, l'attività di accertamento è stata svolta da ufficiali di polizia giudiziaria appartenenti al Nucleo Crimini Informatici, con una preparazione e formazione informatica di alto livello. Inoltre, sia le tracce informatiche che il funzionamento del worm sono stati confermati dallo stesso imputato, pertanto non si vede come possa essere messa in discussione una concordanza tra le prove documentali e le ammissioni dell'imputato.

E' stata invece riconosciuta l'assenza delle aggravanti all'art.615-ter c.p., poiché il funzionamento di Vierika non danneggia i programmi dell'utente, i quali rimangono allo stesso livello operativo, con le stesse caratteristiche e gli stessi scopi. Il worm si limita ad utilizzare tali programmi, senza modificarne il funzionamento.

La fattispecie di alterazione del sistema punita all'art. 615-quinquies c.p., risulta invece presente, confermando la sentenza di condanna di primo grado. Non può altro che essere definita come alterazione, l'azione occulta e indesiderata di modifica del registro di Windows. Attraverso un comando del programma, Vierika cambia la home page predefinita del browser e abbassa al livello minimo le protezioni. Viene definita come alterazione di funzionamento, anche l'invio indesiderato di mail a scopo diffusivo del worm.

La Corte d'Appello ritiene quindi l'imputato responsabile del reato all'art. 615-quinquies c.p., determinando la pena a due mesi di reclusione e euro 2000, sostituendo la pena detentiva con la corrispondente pena pecuniaria di euro 2280.

3.4 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche

Art. 617-quater - Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

L'art 617-quater del Codice Penale è inserito nel Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione V "dei delitti contro l'inviolabilità dei segreti". La normativa è indirizzata all'impedimento dell'intercettazione fraudolenta, che si verifica quando si prende conoscenza di comunicazioni altrui, in modo occulto e senza autorizzazione. Il dolo è generico in quanto non è previsto un elemento essenziale che determina la fattispecie, oltre alla volontà del soggetto. La procedibilità del reato è a querela della persona offesa, salvo le aggravanti previste nell'articolo. Oltre a quelle generali, che si configurano quando chi commette il reato lo fa nei confronti di sistemi di pubblica necessità oppure con abuso della qualità di operatore del sistema, è prevista l'aggravante di chi commette il reato esercitando abusivamente la professione di investigatore privato. L'articolo in questione, così come l'art. 617-quinquies c.p. e 617-sexies c.p. che saranno successivamente analizzati, si riferiscono a comunicazioni informatiche in cui si ha una precisa identificazione del destinatario ed esiste quindi una corrispondenza inviolabile (es. e-mail, chat dirette ad un utente specifico). Nei casi in cui i destinatari non sono definibili, come nei siti o nelle chat pubbliche, i reati sopra indica-

ti non sussistono. Si ritiene importante specificare la differenza tra i termini enunciati nell'articolo:

intercettazione, si ha quando il messaggio giunge integralmente al destinatario;

interruzione, si ha quando l'invio del messaggio viene interrotto e pertanto non giunge al destinatario;

impedimento, si ha quando il messaggio non riesce nemmeno a partire.

Lo "sniffing" è una tecnica che ha lo scopo di intercettare dati e informazioni che attraversano la rete. Si tratta quindi di un'azione che pone in essere il reato di cui all'art. 617-quater. Dal punto di vista difensivo, una soluzione è quella di utilizzare tecniche crittografiche, le quali rendono illeggibile il contenuto dei documenti a chi non ha l'autorizzazione di lettura. Tale azione è molto importante soprattutto per le informazioni sensibili, come possono essere le password o i dati personali. La crittografia più efficace è quella asimmetrica, usata anche nell'implementazione della firma digitale. La crittografia asimmetrica è detta anche "a doppia chiave" in quanto sono utilizzate due chiavi diverse, una privata e una pubblica, le quali funzionano solo congiuntamente. L'illeggibilità del documento nei confronti di terze persone, consiste nell'azione di cifratura che il mittente esegue sul documento con la chiave pubblica del destinatario. A questo punto per poterlo leggere, il destinatario decifra il documento attraverso la propria chiave privata.

3.4.1 Caso giuridico

La sentenza esaminata di seguito riguarda sia l'art. 617-quater c.p. che l'art. 617-quinquies c.p., quest'ultimo analizzato nel paragrafo successivo.

- Tribunale Monza
- 05/03/2012
- Numero 8

L'imputata è stata citata in giudizio per i seguenti capi d'accusa:
artt. 617-quinquies c.p. e 617-quater c.p., per aver installato abusivamente all'interno di apparecchi Pos Setefi, posti alle casse di un negozio, carte di memoria idonee all'intercettazione e registrazione dei codici di accesso di carte di credito, bancomat e simili inseriti dai clienti, per una successiva clonazione,

art. 615-quater c.p., perché con la condotta al capo precedente, effettuava azioni idonee all'accesso abusivo ad un sistema informatico e a falsificare carte abilitate al prelievo di denaro contante, non riuscendo nell'intento per cause indipendenti dalla sua volontà,

art. 635 c.p., per aver danneggiato apparecchi Pos Setefi presenti nel negozio.

Il fatto in questione si è svolto nel seguente modo. Una mattina, prima dell'apertura del negozio, la signora addetta alle pulizie ha trovato nascosta in un camerino una ragazza, la quale aveva presumibilmente passato la notte all'interno del centro commerciale. Sono stati pertanto chiamati, sia la responsabile di negozio che i Carabinieri. Con un primo giro all'interno del negozio tutto sembrava in ordine, salvo poi constatare che gli apparecchi Pos erano stati manomessi. Le apparecchiature sono state quindi consegnate alla ditta che le aveva installate, con l'incarico di esaminarle e riferire quanto riscontrato. Nei giorni successivi è poi emerso che dipendenti e clienti, i quali avevano effettuato acquisti all'interno del negozio, avevano subito la clonazione dei propri bancomat. Il testimone che ha svolto l'analisi tecnica sui dispositivi, ha spiegato che prima dell'analisi interna è necessario effettuare una stampa di un documento contenente i codici identificativi del Pos, e poi esaminare l'apparato esternamente per verificare eventuali segni di effrazione e/o contraffazione. L'esame dell'interno ha permesso di verificare che quattro dei sei Pos erano stati effettivamente manomessi. In particolare presentavano segni di manomissione sulla scheda madre. I Pos sono costituiti da microswitch, ovvero componenti di sicurezza che, all'apertura dell'apparecchio, cancellano la memoria e rendono l'apparato inservibile. Tali componenti erano stati bloccati in modo da non cancellare i dati dei bancomat, mediante un'alterazione dei sigilli di protezione e della scocca, praticandovi un foro per accedervi. A questo punto è stato possibile aprire il Pos, alterarne i circuiti e successivamente richiuderlo. La perizia tecnica conferma, però, di non aver trovato all'interno dispositivi estranei, idonei a memorizzare i dati dei bancomat. La mancata rilevazione di una carta di memoria è stata spiegata dall'imputata, la quale ha ammesso di averla nascosta all'interno del negozio, prima del suo ritrovamento. La stessa ha inoltre esposto il comportamento criminoso nel suo insieme, che si divide in tre parti. La prima parte consiste nell'introdursi all'interno del negozio, inserire una carta di memoria nelle apparecchiature Pos e nascondersi fino all'apertura del giorno seguente. La seconda, consiste nel tornare due settimane dopo per riprendere la carta di memoria, con le stesse modalità. Infine tali carte dovevano essere consegnate a soggetti che ne avrebbero estrapolato il contenuto, al fine di recuperare i dati delle carte dei clienti, usate nelle due settimane precedenti. Non vi è dubbio circa la responsabilità dell'imputata in merito ai

fatti sopra esposti tranne che per l'ultima fase, la quale non si è concretizzata solo per cause indipendenti dalla sua volontà, ovvero l'essere stata scoperta. Le condotte dell'imputata integrano le violazioni degli artt. 617-quinquies c.p., 617-quater c.p., 615-quater c.p. e 635 c.p.. Il reato all'art. 617-quater c.p. è però procedibile a querela della persona offesa, che nel caso in esame risulta essere la società Setefi S.p.a. e la società del negozio di abbigliamento. La querela doveva essere presentata dal legale rappresentate di una delle due aziende, e non dalla responsabile di negozio così come è avvenuto. Pertanto l'imputata risulta prosciolta dall'accusa relativa alla violazione dell'art. 617-quater c.p. per difetto di querela, e non perché il fatto non sussista. Un'analoga considerazione va svolta in merito all'art. 635 c.p., poiché gli apparati Pos oggetto di danneggiamento non erano di proprietà pubblica e pertanto, non sussiste l'aggravante per la quale la fattispecie è procedibile d'ufficio. Come per l'art. 617-quater c.p. si ha quindi difetto di querela. L'imputata è stata quindi dichiarata colpevole dei reati di cui agli artt. 617-quinquies c.p. e 615-quater c.p., con pena complessiva di un anno e due mesi di reclusione, più il pagamento delle spese processuali.

3.5 Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche

Art. 617-quinquies - Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617- quater.

L'art 617-quinquies del Codice Penale è inserito nel Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione V "dei delitti contro l'inviolabilità dei segreti". La disposizione configura un reato di pericolo, che sanziona la semplice predisposizione di apparecchiature idonee ad intercettare, impedire o interrompere comunicazioni informatiche. Il reato risulta pertanto configurabile anche quando si riscontra l'installazione di tali dispositivi, senza la necessità di verificare la memorizzazione o utilizzazione delle comunicazioni intercettate. Nel caso in cui avvenga l'effettiva intercettazione, interruzione o impedimento, si procederà in base alle disposizioni dell'art. 617-quater.

Si ritiene importante considerare una pronuncia da parte del GIP di Milano, del 19/02/2007 riguardo tale normativa: "integra il reato di cui all'art. 617-quinquies c.p. e non il reato di cui all'art. 615-quater c.p. la condotta di chi installa su uno sportello bancomat, in sostituzione del pannello originario, una apparecchiatura composta da una superficie plastificata, con una microtelecamera con funzioni di registratore video per la rilevazione dei codici bancomat, quando non vi sia prova certa dell'avvenuta captazione di almeno un codice identificativo. L'attività illecita di intercettazione, infatti, nel silenzio dell'art. 617-quinquies c.p., deve ritenersi possa essere consumata con qualunque mezzo ritenuto idoneo a svelare la conoscenza di un sistema informatico quale è da considerarsi la digitazione da parte dell'operatore umano del codice di accesso ad un sistema attraverso una tastiera alfanumerica, digitazione che era destinata ad essere l'oggetto dell'illecita captazione". Riflettendo sulla massima del GIP di Milano, si possono trovare diverse motivazioni riguardo questa scelta. L'art. 615-quater c.p. è anch'esso un reato di pericolo ma di dolo specifico, pertanto se la condotta non provocasse un profitto o comunque un danno a terzi il reato non sussisterebbe. L'art. 617-quinquies c.p. risulta punire una fattispecie più ampia di condotte, dove comunque si ha anche un'installazio-

ne di apparecchiature non prevista dall'art. 615-quater. Quest'ultimo parla di codici, parole chiave o mezzi idonei all'accesso ad un sistema informatico, i quali vengono considerati dall'art. 617-quinquies come una comunicazione relativa ad un sistema informatico.

3.5.1 Caso giuridico

Di seguito sono esaminati due casi piuttosto simili, relativi all'art. 617-quinquies c.p..

CASO 1

- Tribunale Trento
- 10/03/2014
- Numero 256

Gli imputati di questo caso sono tre e sono stati citati in giudizio per aver, in concorso tra loro, posto in essere i seguenti reati:

art. 617-quinquies c.p., per aver installato apparecchiature atte a intercettare, impedire e interrompere comunicazioni relative al sistema telematico bancario e postale. Tale attività è stata svolta in tre diversi sportelli, due di tipo bancario e uno postale. Si rileva l'aggravante, in quanto il danno è stato effettuato su sistemi utilizzati da imprese che erogano servizi di pubblica utilità;

art. 55 Dl.vo 231/2007, perché al fine di trarne profitto veniva usata indebitamente una tessera bancomat clonata, effettuando tre prelievi dell'importo totale di mille euro.

Dalle indagini è emerso che gli impiegati di un primo istituto di credito hanno segnalato ai Carabinieri la manomissione degli sportelli bancomat della loro filiale. Questi ultimi, una volta sul posto, hanno verificato l'inserimento di una placchetta di plastica all'interno della bocchetta per l'inserimento delle tessere, impedendo appunto di poter introdurre il bancomat. Gli stessi Carabinieri hanno poi notato la presenza nei pressi delle filiale di due individui sospetti, sulla cui auto sono stati rinvenuti e sequestrati un cacciavite, un tubetto di colla e diverse carte magnetiche di tipo bancomat. Dall'analisi dei filmati delle videocamere di sorveglianza, si sono potuti riconoscere i tre odierni imputati, nell'atto di armeggiare in modo sospetto nello sportello. Il giorno successivo è stata ricevuta la segnalazione, da parte del responsabile

dello sportello "postamat" di Poste Italiane ubicato nelle vicinanze dell'istituto di credito precedente, circa l'apposizione di una tastiera e di un lettore. Dopo aver visionato i filmati delle telecamere è stato possibile riconoscere gli stessi soggetti del giorno precedente, che apponevano congegni atti alla clonazione dei bancomat, che più tardi erano tornati a togliere. Successivamente è stata anche recepita una denuncia di una cittadina, a cui erano stati sottratti circa mille euro dal proprio conto corrente, probabilmente in seguito alla clonazione del proprio bancomat. La testimone ha raccontato di aver effettuato un prelievo da un terzo istituto di credito, sempre nelle vicinanze dei primi due, pertanto sono stati visionati anche i filmati di tale sportello. Da questi si vedeva chiaramente uno degli imputati installare i congegni incriminati, salvo poi rimuoverli dopo poche ore. Da questi fatti è stato possibile stabilire la strategia dei malviventi che consisteva nel bloccare lo sportello del primo istituito di credito esaminato, inducendo così i clienti a effettuare prelievi negli altri sportelli vicini, su cui erano stati installati i dispositivi di clonazione. La mancanza di denunce di prelevamenti agli sportelli relativi al primo istituto di credito e allo sportello postale, non fanno decadere il reato previsto dall'art. 617-quinquies c.p., in quanto quest'ultimo è un reato di pericolo che si consuma con la sola installazione di apparecchiature elettroniche per la clonazione, senza che sia necessario accertare l'effettiva memorizzazione e utilizzazione dei dati illecitamente procurati. Sussiste anche il reato punito dall'art. 55 Dl.vo 231/2007, essendo accertata l'utilizzazione dei dati della tessera bancomat della testimone. Per tutti i motivi sopra elencati, si afferma la responsabilità di tutti e tre gli imputati per i reati analizzati, per i quali ricorre il vincolo di continuità essendo il primo effettuato per poter commettere il secondo. Gli imputati sono stati condannati alla pena di anni uno e mesi sei di reclusione, più il pagamento di mille euro per ciascun imputato, oltre alle spese processuali.

CASO 2

- Corte appello Trento
- 16/01/2015
- Numero 371

Anche in questo caso gli imputati sono tre e sono stati chiamati in giudizio per aver effettuato azioni similari al caso precedente, per di più sullo sportello dello stesso istituto di credito della stessa città. Gli imputati sono considerati responsabili dei seguenti reati:

art. 617-quinquies c.p. e 640-ter c.p., per aver inserito nella postazione bancomat di un istituto di credito due congegni idonei ad alterare il funzionamento dell'apparecchiatura bancomat e per così acquisire, abusivamente, i codici segreti della clientela. Il fine ultimo sarebbe stato quello di effettuare prelievi tramite le carte clonate, scopo non realizzato a causa della scoperta del meccanismo fraudolento.

I due congegni erano costituiti da uno skimmer per la lettura di carte di credito a banda magnetica e successiva memorizzazione dei codici digitati, ed un videosistema idoneo a intercettare e memorizzare i pin digitati sul tastierino numerico, puntato dal dispositivo. La sentenza del Tribunale di Rovereto del 10/01/2013, condannava due imputati alla reclusione di un anno e un mese, e il terzo alla reclusione di un anno e cinque mesi. La maggiore pena di quest'ultimo è derivata dalla rilevazione delle sue impronte sullo sportello incriminato. I fatti si sono svolti nell'ottobre del 2008 quando, durante un semplice pattugliamento, i Carabinieri hanno controllato e identificato tre soggetti all'interno di una macchina, nel piazzale antistante l'istituto di credito. Nella stessa mattina i Carabinieri erano stati poi chiamati dal direttore della filiale, per aver notato tre soggetti armeggiare nei pressi del bancomat. Visionando i filmati della telecamera di sorveglianza si è potuto riconoscere, senza ombra di dubbio, i tre soggetti identificati in precedenza a bordo dell'auto. I tre imputati sono stati ritenuti pertanto colpevoli di entrambi i reati. Il reato di cui all'art. 617-quinquies c.p. si è perfezionato in quanto, trattandosi di un reato di pericolo, non è necessario verificare l'effettiva memorizzazione e utilizzazione dei dati illecitamente procurati. Anche il tentativo di frode informatica, di cui all'art. 640-ter c.p., è integrato poiché l'installazione degli apparecchi era sicuramente finalizzata ad effettuare successivi prelievi, resi impossibili per l'intervento delle forze dell'ordine. La sentenza è stata successivamente impugnata per diverse cause. La prima motivazione riguarda l'errata individuazione dei responsabili del fatto, la seconda consiste in un difetto di querela dell'art. 640-ter c.p., la terza nella mancata consumazione del fatto di cui all'art. 617-quinquies c.p.. La Corte d'Appello ha confermato la sentenza impugnata condannando l'appellante al pagamento delle spese processuali, per i motivi di seguito analizzati. Non vi è alcun dubbio circa l'individuazione dei responsabili, in quanto i Carabinieri hanno avuto modo sia di vederli da vicino al momento dell'ispezione nell'auto, sia di riconoscerli successivamente nei filmati della telecamera di sicurezza. Inoltre, per uno dei tre imputati, sono state trovate le impronte nello sportello bancomat. Anche il difetto di querela non sussiste, avendo il direttore di filiale la qualità di institore, dotato del potere di compiere gli atti giuridici inerenti l'impresa, compreso sporgere querela per fatti inerenti l'operatività della stessa. Infine, come già detto in precedenza, l'art.

617-quinquies c.p. si è consumato, in quanto essendo un reato di pericolo non è necessario verificare che le apparecchiature installate abbiano effettivamente memorizzato dati illecitamente.

Si ritiene sia necessaria una piccola riflessione riguardo l'applicazione dell'art. 55 Dl.vo 231/2007 nel primo caso analizzato, e dell'art. 640-ter c.p. nel secondo caso. Come sarà spiegato nel paragrafo sulla frode informatica, la Cassazione si è espressa nel seguente modo: "integra il delitto di frode informatica e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi" *(Cassazione Penale, sez. II, sentenza n. 17748 del 15/04/2011, Rv.237175).*

3.6 Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche

Art. 617-sexies - Chiunque, al fine di procurare a sè o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.

L'art 617-sexies del Codice Penale è inserito nel Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione V "dei delitti contro l'inviolabilità dei segreti". La normativa sanziona il comportamento di chi falsifica, altera o sopprime il contenuto di comunicazioni informatiche. Per la configurazione del reato si ha oltre al dolo generico, che consiste nella volontà di falsificare il contenuto di una comunicazione informatica, anche il dolo specifico, caratterizzato dal fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno. Inoltre, poiché il reato sussista, è necessario che l'agente utilizzi tali comunicazioni falsate, o ne faccia un uso illegittimo permettendone ad altri l'uso. L'art. 617-sexies c.p. mira quindi a punire l'impiego e la rivelazione pubblica dei contenuti falsati, alterati o soppressi a scopo di profitto o a danno di altri.

3.6.1 Caso giuridico

Relativamente a questo reato informatico, si è deciso di analizzare tre diversi casi, ciascuno con pronuncia da parte della Cassazione Penale. Le motivazioni che hanno spinto al ricorso in terzo grado riguardano solo marginalmente le norme che disciplinano l'ambito informatico. Si è stabilito di analizzare solo queste, lasciando a margine i fatti concernenti temi non oggetto di questa tesi.

CASO 1

- Cassazione penale sez. V
- 18/12/2012
- Numero 18497

Nel caso in esame, l'imputato è stato ritenuto responsabile dei reati di cui agli artt. 615-ter c.p. e 617-sexies c.p., per essersi introdotto abusivamente nel sistema informatico della Telecom Italia S.p.a. e averne falsificato l'indirizzo e-mail. Il fine di queste azioni era quello di arrecare danno alla suddetta società. Infatti, lo stesso è stato condannato ai sensi dell'art. 595 c.p., per aver offeso la reputazione della Telecom Italia S.p.a. inviando un gran numero di messaggi spamming contenenti fatti diffamatori, come se li avesse spediti la società stessa. L'imputato è stato condannato in merito a questi reati, sia dal Tribunale di Roma il 23/04/2009, che in secondo grado dalla Corte d'Appello di Roma il 14/04/2010, la quale ha confermato la sentenza di primo grado. Il ricorso è stato presentato con tre diverse motivazioni, una per ogni reato contestato. Si è deciso di esaminare le due motivazioni in merito alle norme informatiche. Per quanto riguarda l'art. 615-ter c.p., il ricorso è stato presentato per presunta mancanza dell'elemento oggettivo costituente il reato, ovvero l'esistenza di un sistema protetto da misure di sicurezza, e anche per la presunta mancanza dell'elemento soggettivo, ovvero la volontà dell'imputato di realizzare la condotta specificata dalla norma. La Cassazione ha rilevato sia la presenza dell'elemento oggettivo che di quello soggettivo. Invero, secondo un orientamento giurisprudenziale, la violazione dei dispositivi di protezione di un sistema informatico non ha rilevanza di per sé, perché non si tratta di un illecito di effrazione, ma solo come comportamento contrario alla volontà del proprietario del sistema, che ne dispone legittimamente. D'altra parte, la presenza dell'elemento soggettivo è evidente, in quanto l'imputato ha consapevolmente violato il sistema allo scopo prefissato di polemica contro l'impresa di comunicazioni. Il ricorso relativamente all'art. 617-sexies c.p. è stato presentato per mancata dimostrazione dell'avvenuta intercettazione di comunicazioni appartenenti a Telecom Italia S.p.a.. Anche questa doglianza non è valida, in quanto la norma tutela la corrispondenza informatica e punisce la contraffazione del contenuto delle comunicazioni relative ad un sistema. Il fine è quello di garantire la veridicità delle comunicazioni e impedire che possano essere usate comunicazioni false a proprio vantaggio. Il reato risulta pertanto configurabile, in quanto l'imputato, senza autorizzazione, ha creato un messaggio nascondendo la propria identità, e facendolo apparire come inviato dalla società danneggiata, realizzando così una vera e propria contraffazione. Le argomentazioni proposte sono evidentemente infondate e comportano la dichiarazione di inammissibilità del ricorso. Il ricorrente è stato condannato al pagamento delle spese processuali.

CASO 2

- Cassazione penale sez. III

- 12/12/2006
- Numero 5322

Il caso che sarà esaminato è stato portato all'ascolto della Cassazione, in seguito al decreto disposto dal Procuratore della Repubblica di Bolzano. Quest'ultimo in data 08/02/2006 ha richiesto il sequestro di centocinquanta macchine elettroniche da gioco. Questo nell'ambito del procedimento penale a carico di due imputati, indagati per i reati di cui agli artt. 640-ter c.p. e 617-sexies c.p.. Il fatto criminoso consiste nell'essersi procurati un ingiusto profitto, sottraendosi al pagamento dell'imposta dovuta sul totale degli incassi derivanti dalle giocate effettuate sulle apparecchiature di intrattenimento. Tale sottrazione ha prodotto un pari danno nei confronti dell'Amministrazione Autonoma dei Monopoli di Stato, indotti in errore attraverso la manipolazione dei dati contabili delle suddette apparecchiature e conseguente trasmissione dei dati alterati. Ciò è stato reso possibile sostituendo le schede delle apparecchiature, o comunque modificandole per mezzo di appositi programmi software, che ne abbassavano il numero delle giocate, diminuendo falsamente la somma sulla quale deve essere calcolata l'imposta. Uno degli imputati, amministratore della società coinvolta, ha inoltre comunicato falsamente che 50 di queste apparecchiature si trovassero in magazzino, quando invece erano installate e funzionanti presso gli esercizi pubblici. Per quanto riguarda l'art. 617-sexies c.p., oggetto di questo paragrafo, questo risulta configurato in quanto gli imputati hanno ottenuto un ingiusto profitto a danno dell'Amministrazione dei Monopoli di Stato, falsando le comunicazioni relative al sistema informatico. Le motivazioni del ricorso in Cassazione non riguardano le norme informatiche, ma modalità sul sequestro delle apparecchiature e omessa motivazione dell'urgenza del sequestro, pertanto non saranno analizzate. Per completezza, si informa che il ricorso è risultato valido e la Corte Suprema di Cassazione ha annullato l'ordinanza impugnata, con rinvio al Tribunale di Bolzano.

CASO 3

- Cassazione penale sez. II
- 17/10/2007
- Numero 47389

Il caso riguarda un imputato che, nella sua figura di consulente fiscale, ha indotto un dipendente dell'Agenzia delle Entrate di Palermo a introdursi abusivamente nei sistemi informatici dell'amministrazione. Successivamente all'accesso abusivo, il dipendente ha falsato le informazioni relative a crediti

dell'Erario nei confronti dei clienti dell'imputato. In questo modo, i beneficiari di questi falsi sgravi fiscali hanno ottenuto un ingiusto profitto, pari all'importo complessivo di circa cinquantamila euro. In seguito ad una ricostruzione dei fatti, anche in un contesto temporale più ampio, sono state verificate circa duecentocinquanta frodi informatiche con un danno per l'Amministrazione di circa un milione e cinquecentomila euro. Il Tribunale di Palermo contestava che le condotte dovessero integrare il reato di cui all'art. 617-sexies c.p., e non quelli di cui agli artt. 615-ter c.p. e 640-ter c.p., dato che la condotta è consistita nell'aver falsificato dei documenti della pubblica amministrazione ed aver ottenuto un ingiusto profitto con danno altrui. La responsabilità dell'imputato è evidente, in quanto coloro che hanno beneficiato degli sgravi fiscali erano suoi clienti. Inoltre lo stesso coimputato, dipendente dell'Agenzia delle Entrate, ha ammesso le proprie responsabilità richiamando in causa l'imputato. Ha infatti testimoniato di aver da lui ricevuto le cartelle esattoriali dei beneficiari, insieme ad una tangente del 10 per cento per la propria attività illecita. Il Tribunale di Palermo si è espresso in data 01/06/2007, disponendo gli arresti domiciliari nei confronti dell'imputato. Come per il caso precedentemente analizzato, anche in questo i motivi di ricorso in Cassazione non riguardando le norme informatiche, e pertanto non saranno analizzati. La Cassazione ha comunque rigettato il ricorso e condannato il ricorrente al pagamento delle spese processuali.

3.7 Danneggiamento di informazioni, dati e programmi informatici

Art. 635-bis – 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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

L'art 635-bis del Codice Penale è inserito nel Titolo XIII "dei delitti contro il patrimonio", Capo I "dei delitti contro il patrimonio mediante violenza alle cose o alle persone". Rispetto all'art. 615-quinquies c.p., che si pone come norma di sbarramento preventiva costituendo un reato di pericolo, gli artt. 635-bis e seguenti sono dei reati di danno. La prima punisce la diffusione di strumenti atti a danneggiare un sistema informatico, i secondi puniscono il danneggiamento vero e proprio. Il reato è stato originariamente introdotto dalla legge del 1993 con l'art. 635-bis c.p., il quale sanzionava il danneggiamento dei sistemi informatici e informazioni, dati e programmi informatici. La legge del 2008, di ratifica alla Convenzione sulla criminalità informatica, ha rafforzato e specializzato le norme sanzionatorie. Attualmente si può fare riferimento a quattro diversi articoli, che per comodità di analisi, sono esaminati all'interno di questo unico paragrafo.

art. 635-bis c.p. danneggiamento di informazioni, dati e programmi informatici.

art. 635-ter c.p. danneggiamento di informazioni, dati e programmi informatici di pubblica utilità.

art. 635-quater c.p. danneggiamento di sistemi informatici o telematici.

art. 635-quinquies c.p. danneggiamento di sistemi informatici o telematici di pubblica utilità.

La legge n. 48 del 2008 ha pertanto scorporato e specializzato la norma preesistente in due norme diverse, con l'aggiunta di ulteriori due norme che prevedono le aggravanti sul danneggiamento di informazioni o sistemi dello Stato, di un ente o comunque di pubblica utilità. Per quanto riguarda l'analisi

relativa all'art. 635-bis c.p., i comportamenti in origine puniti erano quelli di "distruzione" e "deterioramento", il primo inteso come danneggiamento materiale, il secondo come danneggiamento informatico, ad esempio attraverso l'impiego di malware. Con la modifica del 2008, sono state aggiunte le condotte di "cancellazione", "alterazione", "soppressione", allo scopo non tanto di renderle distinguibili, quanto di assicurare una totale copertura relativa al danneggiamento. Comportamenti punibili dall'art. 635-bis c.p. sono lo spamming e il netstrike. Lo spamming consiste nell'invio di messaggi indesiderati, anche detti "posta spazzatura". Il netstrike si ha con contemporanei e ripetuti accessi da parte di moltissimi utenti ad un sito Web, fino a renderlo inefficiente. Il reato è procedibile a querela della persona offesa, salvo procedibilità d'ufficio nei casi in cui il reato è posto in essere con violenza o minaccia, o da parte di un operatore di sistema. È stato regolamentato a parte, nell'art. 635-ter c.p., il danneggiamento di informazioni di pubblica utilità, proprio per la natura sensibile di questi dati. L'articolo è stato suddiviso in due commi, dove nel primo si prevede un reato di pericolo, mentre la concreta realizzazione del danneggiamento viene prevista e punita più severamente al secondo comma. Anche per questa norma vengono considerate le fattispecie aggravanti ricordate in precedenza. Per completare le indicazioni della Convenzione di Budapest, si sono aggiunte le due fattispecie dirette a danneggiare non singoli dati e programmi, ma il funzionamento di un sistema informatico. Gli artt. 635-quater c.p. e 635-quinquies c.p., sono stati costruiti allo stesso modo degli artt. 635-bis c.p. e 635-ter c.p., prevedendo uno il danneggiamento di sistemi generali, l'altro di sistemi di pubblica utilità. Tra le condotte sanzionate, oltre al "rendere in tutto o in parte inservibile" il sistema, si persegue anche l'averne "ostacolato gravemente" il funzionamento. Tale fattispecie riguarda azioni che non hanno prodotto in totalità gli effetti verso cui era indirizzata, e non è sempre facilmente osservabile in relazione anche all'art. 615-quinquies, il quale punisce i fatti "diretti a" ostacolare gravemente il funzionamento del sistema.

3.7.1 Caso giuridico

In relazione all'art. 635-bis c.p., si è scelto di analizzare un caso portato in esame alla Cassazione per successivi ricorsi.

- Cassazione penale sez. V
- 18/11/2011
- Numero 8555

Il caso in questione riguarda un contenzioso tra l'impiegato di una ditta individuale e la ditta stessa, in merito al danneggiamento dei dati contenuti nel sistema informatico dell'azienda. Il fatto consiste nella cancellazione, eseguita dall'imputato, di una grande quantità di dati dall'hard disk del personal computer nella sua postazione di lavoro. Inoltre, lo stesso, si è impossessato di diversi cd rom contenenti i back-up successivi al 25/06/2004, sottraendoli pertanto al titolare.

Il giudice di merito, successivamente all'esame dei fatti nel contraddittorio, ha condannato l'imputato alla pena prevista dall'art. 635-bis c.p., relativa al danneggiamento di informazioni, dati e programmi di un sistema informatico. La condanna ha previsto inoltre il risarcimento dei danni a favore della ditta danneggiata, che si è costituita parte civile. Tale sentenza di primo grado pronunciata il 27/11/2009 dal Tribunale di Catania, è stata successivamente confermata dalla Corte d'Appello di Catania il 16/02/2011.

Il legale difensore dell'imputato, il 12/05/2011, ha proposto ricorso in Cassazione per le motivazioni elencate di seguito. Il primo motivo d'impugnazione riguarda una violazione dell'art. 606, lett. b), in relazione ad una presunta errata applicazione dell'art. 635-bis c.p., che porterebbe ad un'insussistenza degli estremi del reato. Il secondo motivo si riferisce ad una violazione dello stesso art. 606, lett. e), per quanto riguarda l'imputazione del soggetto sulla base di dati congetturali. Il terzo motivo del ricorso è una violazione dell'art. 606, lett. c), in base ad una presunta inosservanza delle norme processuali e alla mancanza di una perizia tecnica.

La discussione sulla prima motivazione del ricorso verte sul significato da attribuire alla parola "cancellazione" e sull'effettiva mancanza dei dati. Il tecnico informatico di fiducia richiamato dalla ditta, ha testimoniato di aver recuperato i dati, successivamente alla cancellazione effettuata dall'imputato. Il legale difensore ha ritenuto quindi che il reato non sussistesse, poiché l'art. 635-bis c.p. definisce la cancellazione come rimozione definitiva dei dati dalla memoria del computer. Dal punto di vista concreto, però, lo stesso tecnico ha riferito di aver sì recuperato i file cancellati, ma di non averli aperti e che solo in seguito ad una loro apertura se ne sarebbe potuta verificare l'integrità. Dopo aver ascoltato altri testimoni si è constatato che il tentativo di apertura non ha dato il frutto sperato, in quanto la maggior parte dei file è irrecuperabile. Anche dal punto di vista formale, nel gergo informatico la "cancellazione" consiste nella rimozione di determinati dati in via provvisoria, attraverso il loro spostamento nell'apposito cestino, o in via "definitiva" mediante il successivo svuotamento dello stesso. Le virgolette su "definitiva" sono necessarie in quanto, anche in quel caso, i file possono essere recuperati, ma solo attraverso una complessa procedura tecnica che richiede conoscenze nel campo dell'informatica. È stata quindi ritenuta corretta l'interpretazione della norma da parte

dei giudici di primo e secondo grado, secondo cui si ha cancellazione anche quando i dati sono recuperabili, seppure con tecniche dispendiose. Nel caso in esame l'attività dell'imputato ha prodotto un danno, in quanto il recupero ha comportato spese e l'impiego di tempo lavorativo. Il danneggiamento è stato anche a livello fisico, dato che i file recuperati non potevano essere aperti e sono stati definitivamente persi, probabilmente per un'operazione di sovrascrittura. Il reato all'art. 635-bis c.p. pertanto sussiste.

La seconda ragione d'impugnazione, relativamente alla riferibilità del fatto all'imputato sulla base di congetture, risulta non ammissibile. Lo stesso imputato ha testimoniato l'esistenza di forti tensioni nell'ambito lavorativo e il proprio risentimento, che lo hanno portato alle dimissioni. È stata inoltre verificata l'effettiva manomissione del computer alla sua postazione e che l'impossibile apertura di alcuni file recuperati, era dovuta all'apposizione di password che solo l'imputato stesso conosceva.

Il terzo motivo di ricorso non è pertinente al caso in esame. Non è stata l'autorità a richiedere un'indagine tecnica, la quale nel caso avrebbe certamente dovuto rispettare determinati canoni, ma è stata la ditta danneggiata a richiedere ad un tecnico di fiducia di cercare di recuperare i file cancellati.

Per tutte queste motivazioni il ricorso è stato rigettato, condannando il ricorrente al pagamento delle spese processuali.

3.8 Frode informatica

Art. 640-ter - Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.

La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal n. 1) del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

L'art 640-ter del Codice Penale è inserito nel Titolo XIII "dei delitti contro il patrimonio", Capo II "dei delitti contro il patrimonio mediante frode".Il legislatore, con la legge del 1993, ha voluto estendere la normativa prevista dall'art. 640 c.p. con l'art. 640-ter c.p.. La motivazione risiede nel fatto di dover punire fattispecie di reato che non avrebbero trovato una corrispondenza soddisfacente nel paradigma della truffa. La condotta punita rimane quella di procurarsi un ingiusto profitto con altrui danno, in seguito all'alterazione di un sistema informatico o all'intervento senza diritto sul suo contenuto. La differenza risiede nell'oggetto dell'attività fraudolenta, che non investe la persona ma il sistema informatico. Il soggetto passivo non è quindi la persona umana che viene indotta in errore, ma il sistema che subisce un'illecita alterazione. La specializzazione della norma è stata doverosa da parte del legislatore, poiché un sistema informatico non presenta un aspetto psicologico tale da essere raggirato, ma le condotte che sono effettivamente punite sono quelle di "alterazione" del suo funzionamento e "l'intervento" senza diritto sul suo contenuto, dal quale è possibile trarre profitto con altrui danno. A differenza del reato di truffa che richiede artifici e raggiri, l'"alterazione" può essere effettuata in qualsiasi modo, attraverso modifiche interne o esterne, sia su software che hardware, le quali modificano lo scopo a cui il sistema è destinato. Il reato sussiste anche quando la destinazione del sistema non viene modificata, ma si interviene sul suo contenuto alterandone comunque il funzionamento. Rispetto al reato di accesso abusivo previsto dall'art. 615-ter c.p., per la frode informatica non è necessario che il sistema sia protetto da misure di sicurezza poiché il reato sia configurabile. Il reato è procedibile a querela della persona offesa, ovvero su richiesta del proprietario del sistema informatico, ma si può procedere d'ufficio

nel caso in cui l'agente sia un operatore di sistema, circostanza aggravante prevista dalla norma.

Ci si concentra ora sull'aspetto del profitto. Il reato si configura nel momento in cui viene conseguito un ingiusto profitto, con danno patrimoniale di terzi. Questo può verificarsi contestualmente all'alterazione del sistema, oppure in un tempo successivo. Non è necessario che il profitto sia di natura patrimoniale, ma può avere carattere morale ed essere imputato non solo al soggetto agente, ma anche ad altro soggetto. Deve invece necessariamente esserci un collegamento tra l'azione e il conseguimento del profitto.

Il reato di frode informatica si presta a punire anche la fattispecie prevista dall'art. 624 c.p. riguardo al "furto di informazioni", ovvero alla sottrazione di informazioni da un sistema informatico dalle quali si può trarre un ingiusto profitto. Non si identifica il reato in esame, ma sussiste il reato di truffa, quando il soggetto passivo non è il sistema ma una persona indotta in errore attraverso l'uso di strumenti informatici. Bisogna quindi prestare attenzione al fatto che il sistema informatico sia o meno alterato, e in caso positivo si avrà la specificità di frode informatica. Generalmente il reato si consuma in concorso con altri reati informatici che tutelano beni giuridici diversi. Ne è un esempio l'accesso abusivo che si configura quando si accede illegalmente ad un sistema protetto e sussiste senza la necessità di manipolazione del sistema stesso, requisiti esattamente contrari a quelli predisposti dalla frode informatica. Nel caso in cui la manipolazione al sistema lo abbia danneggiato, sarà inoltre imputabile il reato di danneggiamento di sistemi informatici all'art. 635-bis c.p..

Prima di proseguire con l'analisi di un caso giuridico concreto, si vogliono brevemente anticipare due fattispecie di frode informatica: il dialer e il phishing. Il dialer è un programma che, scaricato sul computer dell'utente, altera i parametri della connessione alla rete, disconnette il modem e collega il computer a numeri telefonici a valore aggiunto. In questo modo il soggetto utilizza connessioni dal costo evidentemente superiore, in modo occulto. Il download del dialer avviene generalmente cliccando su banner o entrando in siti Web e l'addebito del costo si concretizza nella bolletta del proprio gestore, di cui una parte viene poi assegnato al titolare del numero a valore aggiunto. Dì per sé non si tratta di un illecito, ma quest'ultimo risiede nelle modalità con cui il provider scarica il dialer nel sistema. La legge prevede che l'utente debba essere informato chiaramente circa i costi massimi e la durata del servizio, in modo tale che ne sia consapevole al momento dell'accettazione. Il phishing è una frode informatica che sfrutta l'ingegneria sociale, ingannando gli utenti di

un servizio allo scopo di sottrarne i dati identificativi. Si tratta di un'attività di invio massivo di messaggi di posta elettronica che imitano, il più fedelmente possibile, la struttura reale dei messaggi legittimi di fornitori di servizi. Attraverso una scusa, quale può essere un aggiornamento del sistema, si invita l'utente a fornire le proprie informazioni riservate, come ad esempio il numero della carta di credito. Tali informazioni vengono poi usate dal malintenzionato, che si sostituisce così all'utente.

3.8.1 Caso giuridico

Il caso che sarà esaminato di seguito riguarda il reato di frode informatica, in concorso con il reato di accesso abusivo a sistema informatico. Come analizzato in precedenza, i due reati coinvolgono requisiti diversi e pertanto, spesso, risultano entrambi imputabili.

- Tribunale Firenze sez. I
- 13/01/2015
- Numero 5932

I capi di accusa dell'imputato sono i seguenti:
art. 497-bis c.p., per l'aver creato una falsa carta d'identità francese, apparentemente rilasciata dal Comune di Parigi in data 08/04/2008, per commettere i crimini ai seguenti capi,
art. 640 c.p., per aver indotto in errore il personale di Poste Italiane, attraverso l'artificio e il raggiro consistiti nell'assumere una falsa identità, e ottenendo l'ingiusto profitto che consiste nell'apertura di un rapporto bancario intestato alla falsa identità, con la possibilità di usufruire di tutti i servizi bancari come anche la disponibilità di una carta Poste Pay,
art. 615-ter c.p., per l'essersi introdotto abusivamente nel dominio internet di Poste Italiane S.p.a. e essersi fraudolentemente procurato i dati personali, codici identificativi e di accesso all'area home-banking inerenti alla Poste Pay di un altro correntista,
art. 640-ter c.p., poiché in seguito all'essersi introdotto nel dominio di Poste Italiane S.p.a e all'essersi fraudolentemente procurato i dati di un correntista, ha disposto la ricarica di euro 491,00 a favore della Poste Pay a sé intestata.

Il caso in questione ha origine in seguito alla denuncia presentata da un correntista, vittima di un'abusiva riduzione dell'importo di euro 491 dalla propria carta prepagata Poste Pay, in seguito ad un'operazione di ricarica online

della carta Poste Pay dell'imputato. Successivamente a indagini tecniche si è riscontrato che l'operazione è stata effettuata tramite un indirizzo IP tedesco, pertanto le indagini si sono rivolte all'intestatario della carta ricaricata. E' stata acquisita una copia del documento di identità dell'intestatario e, nel corso dell'attività investigativa, si è verificato che l'imputato era già stato arrestato in circostanze simili, per il possesso di un'altra carta d'identità falsificata. In quell'occasione era stata ritrovata in suo possesso anche la carta d'identità oggetto dell'attuale dibattimento. L'imputato non ha riferito una diversa versione dei fatti, confermando le azioni indicate. Innanzitutto si è configurato il reato di accesso abusivo a sistema informatico, all'art. 615-ter c.p., in quanto l'introduzione nel sistema informatico delle Poste Italiane S.p.a. si è realizzata abusivamente, attraverso l'utilizzo di codici di accesso fraudolentemente recuperati. Successivamente è integrato il reato di frode informatica, poiché i dati sono stati utilizzati dall'imputato per trasferire una somma di denaro ricreando un proprio ingiusto profitto a danno altrui. Da sottolineare come si è espressa in merito la giurisprudenza di legittimità:

Cassazione Penale, sez. II, sentenza n. 17748 del 15/04/2011, Rv.237175 "integra il delitto di frode informatica e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi";

Cassazione Penale, sezione II, sentenza n. 9891 del 24/02/2011 Rv. 249675, in motivazione "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"

Cassazione Penale, sezione II, sentenza n. 9891 cit. "integra il reato di frode informatica, e non già soltanto quello di accesso abusivo ad un sistema informatico e telematico, la condotta di introduzione nel sistema informatico delle Poste Italiane s.p.a., mediante l'abusiva utilizzazione dei codici di accesso personale di un correntista e di trasferimento fraudolento, in proprio favore, di somme di denaro depositate sul conto corrente del predetto"

Pertanto, le fattispecie di cui all'art. 615-ter c.p. e 640-ter c.p. coesistono nella condotta dell'imputato, aggravate dal nesso teleologico, di cui all'art. 61 n.2 c.p., in quanto la prima fattispecie è stata posta in essere per realizzare il secondo reato. L'imputato oltre alla creazione della carta d'identità falsificata, ha commesso il reato di truffa, art. 640 c.p., esibendo la suddetta carta e ottenendo l'apertura di un conto bancario.

La sentenza determina la condanna dell'imputato a un anno e otto mesi di reclusione, oltre al pagamento delle spese processuali. Tale sanzione è giustificata da un'evidente preparazione ed organizzazione dell'azione criminosa.

Capitolo 4

I Reati Informatici nel mondo

In questo capitolo sono esaminate le disposizioni dell'Unione Europea in termini di reati informatici. È analizzata la Convenzione sul cybercrime di Budapest e definiti gli stati che la hanno ratificata. Al termine, ci sarà un'esposizione delle normative vigenti nelle zone extra Europa, con maggior occhio di riguardo agli Stati Uniti d'America.

4.1 L'a-territorialità

Le caratteristiche di transnazionalità e immaterialità della rete rendono i reati commessi attraverso Internet più difficili da perseguire. Se poi si considerano i paesi cosiddetti "paradisi fiscali", la perseguibilità diventa ancora più problematica a causa dell'impossibilità per le amministrazioni di polizia di poter ottenere la necessaria collaborazione. Inoltre la rete è sempre stata considerata come un luogo libero, in cui l'anonimato è visto come una garanzia di riservatezza, e non un pericolo per la rete. A differenza dei reati comuni, che sono consumati nel luogo in cui si trova l'autore del reato e hanno per oggetto persone o beni individuabili nella realtà fisica, i reati informatici sono realizzati in uno spazio virtuale in cui gli oggetti del reato sono spesso intangibili. Rispetto al criminale comune, l'agente di un reato informatico ha il vantaggio di poter essere un cittadino straniero, realizzare la propria condotta per mezzo di un terminale all'estero, usare un flusso dati che passa in reti estere. In questi casi le autorità devono ottenere permessi e affrontare diverse problematiche processuali. Inoltre le legislazioni in materia dei vari stati sono disomogenee, e risulta pertanto necessario individuare con esattezza il luogo in cui l'azione viene consumata. Per quanto riguarda lo stato italiano, la Cassazione ha stabilito che il giudice italiano è competente sia nel caso in cui la condotta si sia verificata all'interno dello stato, sia nel caso in cui il crimine sia iniziato all'estero ma si sia concluso con un evento in Italia. Da queste riflessioni risulta

chiaro come sia necessaria una legislazione il più possibile comune, o comunque una cooperazione che permetta di affrontare questi crimini nel miglior modo possibile.

4.2 Convenzioni UE

La criminalità informatica ha la caratteristica di a-territorialità, per cui risulta di fondamentale importanza adottare disposizioni che siano il più possibile conformi tra i vari stati. In territorio europeo, il primo Consiglio d'Europa dedicato al settore Giustizia e affari interni, ma soprattutto ai reati legati all'uso di tecnologie informatiche, risale al 1999 e si è svolto a Tampere. La consapevolezza della rilevanza internazionale del cybercrime si è concretizzata con l'approvazione, da parte del Consiglio d'Europa in data 23 novembre 2001, della cosiddetta Convenzione di Budapest. Quest'ultima rappresenta il primo accordo internazionale sui reati commessi tramite Internet o reti elettroniche. Il trattato è aperto alla firma degli Stati membri e non membri che hanno partecipato alla sua stesura, ma anche all'adesione degli Stati non membri che non sono intervenuti. Tale Convenzione sul cybercrime ha imposto, a tutti gli Stati membri dell'Unione Europea, di adottare misure legislative rivolte alla repressione penale dei nuovi crimini informatici, armonizzando, in questo modo, i diversi ordinamenti giuridici interni e coordinando forme di collaborazione per quanto concerne la raccolta di prove da parte delle autorità. Il trattato è composto da 48 articoli, suddivisi in quattro capitoli. Il capitolo terzo è intitolato "Cooperazione internazionale", a dimostrazione di quanto questa Convenzione abbia lo scopo di unire i vari Stati verso la repressione dei reati informatici. All'articolo 23 vengono esposti i principi generali di tale cooperazione. Il capitolo primo è rivolto alla definizione di termini quali "sistema informatico", "dati informatici", "service provider" e "trasmissione di dati". Il capitolo secondo è il vero fulcro del trattato in quanto definisce i provvedimenti da adottare a livello nazionale. Il termine "cybercrime" viene utilizzato per definire "reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici". Tali reati possono compiersi con attività quali "l'accesso illegale" (art. 2), "le intercettazioni illegali" (art. 3), "interferenze dei dati e dei sistemi (artt. 4-5), "uso improprio di dispositivi" (art. 6.), "frode informatica e falso" (artt. 7-8), "reati connessi alla pornografia infantile" (art. 9), "reati connessi a violazione del diritto d'autore" (art. 10). I reati di cui agli articoli 9 e 10 non sono trattati da questa tesi, ma sono tuttavia rilevanti e per questo sono stati citati. La Convenzione prevede anche, all'art. 12, la responsabilità delle persone giuridiche quando i crimini informatici siano commessi da persone fisiche allo scopo di far perseguire un vantaggio all'ente

collettivo cui appartengono o di cui sono dipendenti. Alla Convenzione di Budapest hanno presenziato sia Stati dell'Unione Europea che Stati non membri. La situazione al 27 ottobre 2015 vede un totale di 47 Stati, membri e non, che hanno aderito alla Convenzione. Il numero degli Stati che hanno firmato la Convezione, ma alla cui firma non è seguita ratifica sono 7: Andorra, Grecia, Irlanda, Liechtenstein, Monaco, Svezia e, tra gli Stati non membri il Sud Africa. Gli Stati che fanno parte dell'Unione Europea, ma che non hanno né firmato né ratificato la Convenzione sono Russia e San Marino. In ordine di tempo, gli ultimi ad aver ratificato la Convenzione nel 2015 sono Polonia, Turchia e, tra gli Stati non membri, Canada e Sri Lanka. Per quanto riguarda gli Stati Uniti d'America, hanno presenziato e firmato la Convenzione nel 2001, ma l'adesione si è concretizzata con la ratifica il 29 settembre 2006, con entrata in vigore nel 2007. L'Italia ha aderito con la legge n.48 del 2008, che ha aggiornato le disposizioni della legge 547/93.

Si ritiene importante citare la "Decisione quadro relativa agli attacchi ai sistemi d'informazione", enunciata dal Consiglio dell'Unione Europea il 24 febbraio 2005. L'art. 10 denominato "Competenza giurisdizionale", si pronuncia così: "Qualora un reato rientri nella competenza giurisdizionale di più di uno Stato membro e quando ciascuno degli Stati interessati potrebbe validamente avviare un'azione penale sulla base degli stessi fatti, gli Stati membri interessati cooperano per decidere quale di essi perseguirà gli autori del reato allo scopo, se possibile, di concentrare i procedimenti in un solo Stato membro. A tal fine, gli Stati membri possono avvalersi di qualsiasi organismo o meccanismo istituito all'interno dell'Unione europea per agevolare la cooperazione tra le loro autorità giudiziarie ed il coordinamento del loro operato". Il Consiglio Europeo ha inoltre emanato la direttiva 2013/40/UE che sviluppa e sostituisce la decisione quadro 2005/222/GAI del Consiglio, relativa agli attacchi contro i sistemi informatici. Tale direttiva è entrata in vigore il 3 settembre 2013.

Per quanto riguarda il diritto internazionale, il principio di stretta territorialità cede il posto a quello di ultraterritorialità[1]. Questa disposizione potrebbe essere la giusta risposta per dissuadere i criminali informatici, i quali agiscono con la convinzione di non poter essere sanzionati grazie all'applicazione del principio di territorialità. La "globalizzazione del crimine" richiede una "globalizzazione della giustizia", in modo tale da consentire alle autorità di reprimere la criminalità informatica transnazionale.

[1]Piccinni MarioLeone, Vaciago Giuseppe, *"Computer Crimes - Casi pratici e metodologie investigative dei reati informatici"*, pag. 67, 2008

4.3 La situazione extra UE

Sia i governi dei paesi sviluppati sia di quelli in via di sviluppo, hanno acquisito consapevolezza circa la crescente minaccia della criminalità informatica sulla sicurezza economica, politica e sugli interessi pubblici. Un esempio è la cooperazione tra gli Stati Uniti e la Cina, i quali sono i due paesi con la maggiore criminalità informatica[2]. Molte organizzazioni hanno già provveduto a stabilire standard globali di legislazione e applicazione delle leggi, sia a livello regionale che su scala internazionale. Il G8 è un gruppo composto dagli otto paesi cosiddetti industrializzati, anche se la situazione attuale è cambiata dal momento della sua formazione. Nel 1997, il G8 rilasciò un comunicato che prevede un piano d'azione per combattere il cybercrime e proteggere i dati e i sistemi da accessi non autorizzati, e inoltre richiede agli stati membri di avere un punto di contatto tra di essi. L'Assemblea Generale delle Nazioni Unite ha adottato due risoluzioni, nel 2000 e nel 2002, contro l'abuso criminale delle tecnologie dell'informazione. L'agenzia specializzata all'interno delle Nazioni Unite, "International Telecommunication Unit" (ITU), ha un ruolo di primo piano nella sicurezza informatica. Nel 2003 ha rilasciato due disposizioni per la lotta contro i reati informatici. L'Asia-Pacific Economic Cooperation (APEC) ha lo scopo di promuovere la cooperazione economica nella regione asiatica. Nel 2002 ha rilasciato la "Cybersecurity Strategy" che delinea, tra le altre cose, la condivisione di informazioni e la cooperazione tra i vari stati. Nel 2002 anche il Commonwealth ha presentato un modello di legge sulla criminalità informatica che attiva la cooperazione internazionale, in conformità con la Convenzione di Budapest. Nel gennaio del 2011, gli Stati Uniti e la Cina si sono per la prima volta impegnati a collaborare su base bilaterale in tema di sicurezza informatica. "Fighting Spam to Build Trust" è stato il primo approccio tra questi due stati.

Come già detto in più parti di questo lavoro, tutti i settori vitali dell'economia e della società sono ora strettamente dipendenti dall'uso dei computer e della rete Internet. È da questa situazione che nasce la seguente citazione, direttamente dalla Casa Bianca: "Cyber space is their nervous system – the control system of our country. Cyber space is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work" (The White House,

[2] *International Cybercrime*, https://en.wikipedia.org/, 2015

2003)[3]. Uno dei primi esempi di cybercrime[4] negli Stati Uniti, è stato quando nel 1997 un ragazzo del Massachusetts è entrato intenzionalmente e senza autorizzazione nel sistema informatico dell'aeroporto di Worcester e l'ha estromesso per ore dal controllo della Federal Aviation Authority (FAA). Nel 2000, un ragazzo canadese ha realizzato un attacco di "distributed denial-of-service" (DDoS) nei confronti di grandi siti web tra i quali CNN, Yahoo, eBay, Amazon, Dell Computer. Distributed denial-of-service è un attacco informatico con cui si inviano un gran numero di richieste ad un sistema informatico, in modo tale da esaurirne deliberatamente le risorse. In questo modo tale sistema non è più in grado di erogare normalmente i servizi ai client. Un altro reato informatico è stato realizzato sempre nel 2000 da uno studente delle Filippine che ha rilasciato un virus, denominato "I love You", il quale ha infettato e isolato tra gli altri i computers della Casa Bianca, del Pentagono e dell'FBI. Tale virus ha prodotto danni anche in Europa, infettando ad esempio i sistemi del Parlamento inglese, danese e del governo federale della Svizzera. In tutti questi esempi il sistema informatico costituiva l'oggetto finale da danneggiare, pertanto sarà dato ora un esempio di reato in cui il sistema costituisce lo strumento per commettere l'illecito. Nel 1994 un trentenne di Los Angeles, usando i computer dell'Università della California del Sud, ha realizzato una frode informatica venendo in possesso di ventimila numeri di carte di credito. La prima legge statunitense in materia di crimini informatici è stata emanata dal Congresso nel 1984 attraverso la promulgazione del "Computer Fraud and Abuse Act" (CFAA). Tale legge autorizzava i Servizi Segreti degli Stati Uniti ad essere l'agenzia federale principalmente responsabile per le investigazioni sui reati informatici, in collaborazione con altre organizzazioni. Altre norme promulgate dal Congresso sono state nel 1986 "The Electronic Communications Privacy Act" (ECPA), e nel 1996 "The National Information Infrastructure Protection Act". Quest'ultimo ha realizzato una serie di emendamenti alla norma del 1984. Nel 2003 il Congresso ha emanato "The CAN-SPAM Act" allo scopo di risolvere i problemi legati alle email indesiderate. La norma considera come crimine federale l'invio di email commerciali senza nome di dominio e un valido oggetto. La legislazione contro i reati informatici è costituita da un insieme complesso di norme emanate dal Congresso, direttive presidenziali ma anche programmi di sicurezza informatica, creati all'interno delle varie organizzazioni e dipartimenti federali. All'interno del "Department of Homeland Security" è stata creata nel 2003 la "National Cyber Security Division", mentre dall'FBI è stato istituito l'"Internet Crime Compliant Center (IC3). Quest'ultimo è

[3]All'interno di questa citazione della Casa Bianca, *"Cyber space is their nervous system"*, their si riferisce ai settori vitali dell'economia e della società.

[4]Gli esempi di reati informatici da qui in avanti, sono stati presi dal libro *"Crime Policy in America"*, di Shahid M. Shahidullah

attualmente la principale fonte di informazioni federali in materia di cybercrime. Infine, come ultimo esempio, si considera il "Cyber Crime Center", istituito all'interno del Dipartimento di Difesa nel 2001, il quale è la maggiore organizzazione per la ricerca e la formazione sulla sicurezza informatica.

Conclusioni

L'utilizzo sempre più diffuso di strumenti informatici e telematici nella quotidianità, ha prodotto un vertiginoso aumento dei reati commessi in rete. Ci si trova a fronteggiare casi di frode online, furto d'identità telematica, accessi abusivi ai sistemi informatici, attività atte a danneggiare sistemi informatici e telematici. Questi e altri reati, sono stati ampiamente descritti nel corpo della tesi. Punto saliente di quest'ultima è stato lo studio di casi concreti, che ha permesso di effettuare una ricerca approfondita negli archivi delle sentenze, con la difficoltà di selezionare quelle che più consentivano un'analisi completa del reato in esame.

Dallo svolgimento di questo lavoro si è potuto comprendere come, nonostante i vari sforzi anche in campo internazionale, ci siano diversi livelli di idoneità a combattere tali crimini tra i paesi del mondo. Lo stato italiano solo recentemente si è adeguato alle politiche europee, e presenta una situazione di arretratezza rispetto a potenze quali, ad esempio, gli Stati Uniti d'America. Anche per quanto riguarda l'opinione popolare, si ha ancora una concezione di diverso peso tra un furto concreto e uno effettuato online. Si ritiene che debba essere effettuata una maggiore propaganda di sensibilizzazione nei confronti dei cittadini sul tema dei reati informatici, in modo tale da informarli dei rischi e delle azioni di tutela che è possibile adottare.

Dalla ricerca e dallo studio dei vari casi concreti relativi ai reati esaminati, è emerso come non sempre sia rispettata una seria indagine tecnica dei sistemi informatici, e degli eventuali dati contenuti in essi, oggetti del reato. Un fenomeno eclatante è stato quello del caso "Vierika", dove sono state prese per corrette le prove raccolte e consegnate dallo stesso imputato. Come già detto rispetto all'America, dove si hanno organismi specializzati unicamente all'analisi dei crimini informatici, in Italia non si ha la stessa concezione.

Un'ulteriore riflessione riguarda l'applicazione delle norme informatiche da parte di giudici diversi. Nonostante la ratifica della Convenzione sul cybercrime

di Budapest abbia migliorato e ampliato la portata legislativa, si hanno ancora diverse interpretazioni delle norme informatiche. Una stessa fattispecie reale può portare all'applicazione di norme diverse, nonostante la Cassazione Penale si sia rivolta a favore dell'applicazione dell'una o dell'altra. Nel presente lavoro tale situazione si è verificata durante l'analisi di due diversi casi, in cui per la stessa fattispecie è stata applicata in uno la norma di indebita utilizzazione di carte di credito, e nell'altro il reato di frode informatica[5]. .

Un eventuale sviluppo futuro di questa tesi, potrebbe essere rivolto allo studio delle investigazioni informatiche e delle varie norme che le regolano. Molte sono le affinità tra l'investigazione di crimini informatici e quella tradizionale. Il legislatore ha emanato due leggi che hanno rivoluzionato in primo luogo il Codice Penale, con la L. 547/93, e in seguito quello di Procedura Penale con la L. 48/2008. Anche la L. 547/93 ha modificato il Codice di Procedura Penale, ma è proprio la L. 48/2008 che ha apportato le modifiche più significative, integrando gli articoli che regolamentano la fase della ricerca della prova come Ispezione (art. 244 co. 2 c.p.p.), Perquisizione (art. 247 co. 1bis e 352 co. 1bis c.p.p.) e Sequestro (art. 354 co. 2 c.p.p.). Sono state definite delle "norme in bianco", ovvero sono stati specificati solo gli esiti della procedura senza spiegare come questa debba essere realizzata, rimandando alla comunità scientifica la scelta delle modalità da seguire.

La trattazione aveva l'obiettivo di fornire un quadro d'insieme sul dilagante fenomeno dei crimini informatici, seguito da un'analisi approfondita dei singoli reati. La ricerca e lo studio dei casi reali, ha consentito di concretizzare la normativa teorica, fornendo i vari spunti di riflessione sopra esposti.

[5]I due diversi casi in questione sono quelli descritti al paragrafo 3.5.1 relativi al reato di *"Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche"*

Ringraziamenti

Desidero ricordare tutti coloro che mi hanno aiutato nello sviluppo di questa tesi, sia in maniera diretta che indiretta.

Ringrazio anzitutto la professoressa e mia relatrice Claudia Cevenini, che è sempre stata disponibile e mi ha fornito preziosi consigli per lo svolgimento della tesi.

Di grande aiuto sono stati i miei colleghi, i quali mi hanno aiutato nella revisione finale con suggerimenti e osservazioni: a loro va la mia gratitudine, anche se è mia la responsabilità per ogni errore contenuto in questo lavoro. Più di tutti ringrazio Francesca, per aver affrontato insieme ogni passo di questo percorso, sostenendoci a vicenda nei momenti tristi e festeggiando quelli felici. Ringrazio anche Deca, per aver riletto la tesi e avermi segnalato eventuali errori e discordanze.

È il momento di ringraziare Tania, la migliore amica che si possa avere, la quale mi ha sostenuta e sopportata in ogni momento di sclero di questi tre anni, e non meno importante mi ha aiutata nella scelta del vestito da indossare!

Un ringraziamento speciale va al mio ragazzo Andrea, che mi è stato vicino e ha saputo sdrammatizzare ogni momento di tensione e di difficoltà, facendomi passare felicemente i vari momenti di svago.

In ultimo, ma non per importanza, rivolgo un ringraziamento ai miei genitori per il loro sostegno e per avermi spronata ad andare avanti, nonostante le difficoltà incontrate.

Bibliografia

[1] Destito Vito Sandro, Dezzani Giuseppe, Santoriello Ciro, *Il diritto penale delle nuove tecnologie*, CEDAM Editore, 2007.

[2] Himanen Pekka, *L'etica hacker e lo spirito dell'età dell'informazione*, Feltrinelli Editore, 2003.

[3] Giannantonio Ettore, *L'oggetto giuridico dei reati informatici*, Cass. pen. fasc. 7-8, 2001.

[4] Iaselli Michele, *Reati Informatici: introdotta la confisca come pena accessoria*, http://www.altalex.com/documents/leggi/2013/08/28/reati-informatici-introdotta-la-confisca-come-pena-accessoria, 2013.

[5] Battaglia Salvatore, *Criminalità informatica al tempo di Internet: rapporti tra phishing e riciclaggio*, http://www.altalex.com/documents/news/2014/03/28/criminalita-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio, 2014.

[6] Ufficio dei Trattati, *Convenzione sulla criminalità informatica*, http://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185/, 2015.

[7] Piccinni MarioLeone, Vaciago Giuseppe, *Computer Crimes - Casi pratici e metodologie investigative dei reati informatici*, Moretti Vitali Editori, 2008.

[8] Amato Giuseppe, Destito Vio Sandro, Dezzani Giuseppe, Santoriello Ciro, *I Reati Informatici*, CEDAM Editore, 2010.

[9] La Legge Per Tutti - Portale di informazione e consulenza legale, *Art. 615 quater codice penale: Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*, http://www.laleggepertutti.it/codice-penale/art-615-quater-codice-penale-detenzione-e-diffusione-abusiva-di-codici-di-accesso-a-sistemi-informatici-o-telematici.

[10] Shahid M. Shahidullah, *Crime Policy in America*, University Press of America, 2008.

[11] Cevenini Claudia, *Firme elettroniche e documenti informatici*, http://campus.unibo.it/, 2015.

[12] Cevenini Claudia, *I reati informatici*, http://campus.unibo.it/, 2015.

[13] EUR-Lex, L'accesso al diritto dell'Unione Europea, *Attacchi contro i sistemi informatici*, http://eur-lex.europa.eu/legal-content/IT/ALL/?uri=URISERV:l33193, 2014.

[14] Wikipedia, *International Cybercrime*, https://en.wikipedia.org/, 2015

[15] Cristina Cosentini, *Il principio di legalità in materia penale*, http://www.altalex.com/documents/concorsi/2010/03/12/il-principio-di-legalita-in-materia-penale, 2010