REATI INFORMATICI, CODICE PENALE e REGOLAMENTAZIONE COMUNITARIA

INTRODUZIONE ALLA PROBLEMATICA

I reati informatici, o *computer crimes*, possono essere definiti come il risvolto negativo dello sviluppo tecnologico dell'informatica e della telematica.

Lo sviluppo delle tecnologie informatiche ha permesso di disegnare nuovi scenari da qualche decennio a questa parte.

In un lasso di tempo assai breve, la maggior parte delle attività umane svolte manualmente o attraverso apparecchiature meccaniche, hanno lasciato il passo a ben più efficienti implementazioni digitali.

Si pensi ad esempio agli enormi archivi documentali che, fino a non troppi anni fa, creavano grossi problemi di gestione nonché, soprattutto, di indicizzazione.

Il vantaggio della creazione di database informatici centralizzati ha permesso di risolvere gran parte di questi problemi, velocizzando ed ottimizzando tutte le operazioni di ricerca ed estrazione dati.

Con le tecnologie digitali inoltre l'informazione si svincola dal supporto e, di conseguenza, diventa assai facile poter riprodurre il contenuto indipendentemente dal supporto su cui è memorizzato (sia esso un hard disk, un dvd, un usb drive o altro); da tutto ciò ne deriva anche una estrema facilità in termini di portabilità e trasferimento.

Questa naturale facilità di scambio del dato digitale viene ulteriormente incrementata ed agevolata dallo sviluppo delle reti telematiche, in particolare Internet.

Dal connubio informatica-reti telematiche originano ampie possibilità per la crescita della società.

Da ciò si sviluppano attività quali ad esempio l'e-commerce, l'e-government, l'home-banking, il trading online e tante altre attività che consentono di rendere più efficiente la società, ma al contempo la rendono estremamente *net-centrica*. Con ciò si vuole sottolineare il fatto che la maggior parte delle attività sociali, lavorative e di svago passano oggi attraverso reti telematiche.

Se dunque tutti gli interessi e le attività propositive della società si spostano su Internet, di conseguenza, anche le attività illecite (i cd. reati informatici) ne seguiranno l'evoluzione nelle forme e nelle pratiche. A tal riguardo diventa perciò necessario sviluppare idonee contromisure atte a contrastare, o quantomeno a limitare, il progredire di queste forme di crimine.

Al fine di poter contrastare il sempre crescente aumento dei reati informatici, si rende necessario sviluppare metodologie, pratiche e normative in grado di combatterne gli effetti.

Da un punto di vista pragmatico esistono fondamentalmente due grandi tipologie di pratiche che è possibile adottare per contrastare i computer crimes[1]:

1- **Prevenzione** dei reati (lato utente e lato pubblica sicurezza)

2- **Repressione** dei reati (Codice Penale e disposizioni comunitarie)

Al di là della specificità dei singoli illeciti che è possibile compiere attraverso gli strumenti informatici (che verranno di seguito analizzati), è possibile stilare alcune massime di riferimento per prevenire il compiersi dei reati informatici.

[1] *Nuove tecnologie Nuove criminalità*, <http://www.reportonline.it/modules.php?name=News&file=print&sid=2122>

In prima istanza, la pratica prima, è quella di sensibilizzare e responsabilizzare l'utenza sulle potenzialità ma anche sui rischi cui è possibile incorrere attraverso l'uso degli strumenti informatici.

La scarsa alfabetizzazione dell'utenza Internet circa i pericoli ed i rischi su cui è possibile imbattersi, è forse la causa prima della così ampia diffusione del cyber crime[2], e ciò è specialmente vero in determinati tipi di illeciti.

Sempre "lato utente" esistono poi procedure specifiche che verranno proposte nel prosieguo come possibili soluzioni preventive in relazione a specifici reati informatici.

Anche dal "lato della pubblica sicurezza" (Polizia Postale e delle Comunicazioni) esistono soluzioni in grado di prevenire i reati informatici, o comunque designate a tale scopo.

In tale ambito si pensi ad esempio a tutte quelle pratiche finalizzate al monitoraggio della rete Internet e che spesso vacillano tra il lecito e l'illecito, tra la necessità di garantire la sicurezza (come d'altronde postulato dall'art. 5 della "*Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*") e quella di rispettare la privacy e la riservatezza (art. 8 della medesima convenzione).[3]

Citiamo qui ad esempio le pratiche di *data retention*, la possibilità cioè di poter tenere traccia dei dati inerenti gli spostamenti degli utenti, sia per quanto riguarda la navigazione in rete che per l'utilizzo della posta elettronica.

Nello specifico i dati di interesse ai fini della prevenzione sono quelli in grado di identificare la fonte della comunicazione (indirizzo IP) e determinare data, ora e durata della comunicazione (file

---

[2] OCSE, *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione*, <http://www.oecd.org/dataoecd/16/23/15582268.pdf>

[3] *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, <http://www.giustizia.it/pol_internaz/tutela/ce_salv_diritti.htm>

di log) (art. 5 Direttiva 2006/24/CE[4]). In ogni caso comunque tali dati potranno essere conservati per un periodo non superiore a 2 anni (art. 6) e per i soli fini di indagine, accertamento e perseguimento dei reati (art. 1).

I REATI INFORMATICI PREVISTI DAL CODICE PENALE ITALIANO

Prima di analizzare come il Codice Penale classifichi ed individui i computer crimes, è opportuno precisare che per ogni reato previsto si specificheranno anche, oltre alle disposizioni del Codice Penale, le possibilità preventive che l'utenza (intesa sia come utente privato che come azienda) può adottare al fine di scongiurare, al meglio possibile, crimini informatici a proprio danno.

La prima vera normativa contro l'emergente fenomeno dei cyber crimes è stata la legge 547/93 ("*Modificazioni ed integrazioni alle norme del Codice Penale e del codice di procedura penale in tema di criminalità informatica*").

Precedentemente a questa legge molti pochi interventi sono stati fatti in materia di repressione ai reati informatici, soprattutto per quel che riguarda il periodo sino agli anni '90.

Sino ad allora si possono considerare infatti solo casi sporadici, come ad esempio la legge 191/78 che introduceva nel Codice Penale l'art. 420 contro l'attentato ad impianti di elaborazione dati, o la legge 121/81 relativa alla prima forma di tutela dei dati archiviati in un sistema informatico.

A partire dal decennio successivo, con lo sviluppo delle tecnologie informatiche e telematiche, si sente invece una maggior esigenza di dotarsi di leggi più specifiche ed approfondite in materia di tutela informatica, come la legge 197/91 che, all'art. 12 punisce l'indebito utilizzo delle carte di credito o la 518/92 che, con l'art. 10, mira a punire, per vero in maniera eccessivamente generica, i

[4] *Direttiva 2006/24/CE*, <http://www.garanteprivacy.it/garante/document?ID=1485189>

reati di “pirateria informatica”.[5] Ma è con la legge 547/93 che si pongono le basi per una reale lotta al crimine informatico.

Per rendere più agevole la comprensione dei provvedimenti normativi previsti con la suddetta legge, appare conveniente suddividere in macrocategorie le aree di intervento;

1) *Frodi informatiche*;
2) *Falsificazioni*;
3) *Integrità dei dati e dei sistemi informatici*;
4) *Riservatezza dei dati e delle comunicazioni informatiche.*

La macrocategoria delle *frodi informatiche* è regolamentata dall’*art. 640-ter* del Codice Penale, contenuto all’interno del Titolo XIII “dei delitti contro il patrimonio”, Capo II “dei delitti contro il patrimonio mediante frode”, e recita così:

art. 640-ter (“Frode informatica”): **“***Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

[5] *Hacking e criminalità informatica - l’approccio normativo alla criminalità informatica (capitolo III),* <http://www.altrodiritto.unifi.it/devianza/tavassi/nav.htm?cap3.htm>

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."

Si parla qui di un reato consistente nel trarre in inganno un elaboratore elettronico, al fine di ricavarne un guadagno economico (per sé o per altri complici), a danno di un soggetto terzo (solitamente il detentore dell'elaboratore elettronico).

Si tratta perciò di un'estensione del reato di truffa descritto all'art. 640 c.p.

Art. 640 ("Truffa"): "*Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032 .*

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:

1. se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;

2. se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'autorità.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante."

Tra i reati che più frequentemente vengono compiuti, e che ricadono, tra gli altri, all'interno della "frode informatica", vi sono le cd. pratiche di *Phishing* e quelle di diffusione di appositi programmi truffaldini, definiti *Dialer*.

Il phishing altro non è che un'attività finalizzata ad estorcere dati personali (in prevalenza legati alle carte di credito od ai conti bancari) attraverso una richiesta esplicita al suo legittimo possessore. Il principale metodo per porre in essere il phishing è quello di inviare una mail in tutto e per tutto simile a quella che verrebbe inviata da un regolare istituto (banca, sito d'aste, provider,

ecc. e con relativo logo identificativo), nella quale si riportano vari tipi di problemi tecnici (aggiornamento software, scadenza account, ecc.) che motivano l'utente a cliccare sul link riportato nella mail per andare ad aggiornare i propri dati personali.

Chiaramente il link non porta al "vero" sito dell'istituzione, ma ad un sito fasullo ed opportunamente creato dall'autore del reato di phishing, che si impossesserà così dei dati inseriti dall'utente.

Dal punto di vista della prevenzione il phishing si configura come uno di quei reati che possono facilmente essere debellati con una corretta informazione agli utenti.

A tal scopo l'ABI (Associazione Bancaria Italiana) ha stilato una lista di 10 punti chiave nella prevenzione del phishing:

"1. Diffidate di qualunque e-mail che vi richieda l'inserimento di dati riservati riguardanti codici di carte di pagamento, chiavi di accesso al servizio di home banking o altre informazioni personali;
2. è possibile riconoscere le truffe via e-mail con qualche piccola attenzione: generalmente queste e-mail non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati; fanno uso di toni intimidatori; non riportano una data di scadenza per l'invio delle informazioni;
3. nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, non rispondete all'e-mail stessa, ma informate subito la vostra banca tramite;
4. non cliccate su link presenti in e-mail sospette, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale;
5. diffidate inoltre di e-mail con indirizzi web molto lunghi, contenenti caratteri inusuali, quali in particolare @;
6. quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con "https://" e non con "http://" e nella parte in basso a destra della pagina è presente un lucchetto;
7. diffidate se improvvisamente cambia la modalità con la quale vi viene chiesto di inserire i vostri codici di accesso all'home banking;
8. controllate regolarmente gli estratti conto del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la banca e/o l'emittente della carta di credito;
9. le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili

gratuitamente degli aggiornamenti (le cosiddette patch) che incrementano la sicurezza di questi programmi;

10. Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente diffidenti nel consegnare i vostri dati riservati senza essere sicuri dell'identità di chi li sta chiedendo.

In caso di dubbio, rivolgetevi alla vostra banca." [6]

Un altro tipo di reato che rientra nella categoria delle "frodi informatiche" è l'uso del cosiddetto *Dialer*.

Il dialer è un piccolo programma (pochi kilobyte) appositamente scritto per dirottare la connessione Internet dell'ignaro utente verso un altro numero telefonico, spesso di tariffazione internazionale e comunque sempre molto più caro rispetto alla comune chiamata telefonica al numero POP del proprio provider.

Attraverso l'utilizzo del dialer il guadagno è multiplo; operatori di telefonia, società produttrici dei dialer, webmaster.

E' però da precisare che l'utente finale (singolo o azienda che sia) viene colpito dal dialer solo nel momento in cui effettivamente lo scarica e lo installa sul proprio computer. Il dialer infatti è un normalissimo programma e come tale deve preventivamente essere installato per poter essere eseguito.

Una volta installato sarà il dialer che automaticamente sostituirà il numero ordinario di connessione con un numero a tariffazione maggiorata.

Anche per la frode mezzo dialer, come per il phishing, molto importante è l'informazione dell'utenza Internet, la quale può proteggersi da questa truffa attraverso pochi e semplici accorgimenti.

---

[6] *Il phishing: analisi, dati e previsioni*, <http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=545>

Innanzitutto è possibile disabilitare presso il proprio operatore telefonico le chiamate verso numerazioni internazionali e/o verso i numeri speciali a pagamento.

In secondo luogo è possibile installare appositi software (definiti "stop dialer") in grado di avvisare l'utente quando un programma terzo tenta di dirottare la connessione verso un altro numero telefonico non previsto.

Altro provvedimento che è possibile adottare è quello di utilizzare una linea telefonica basata su tecnologia xDSL od a fibra ottica che, effettuando chiamate dirette e verso un solo numero, non subisce alcun danno dai dialer.[7]

La seconda macrocategoria, quella delle *falsificazioni*, è regolamentata dal Codice Penale attraverso l'art. 491-bis contenuto nel Titolo VII "dei delitti contro la fede pubblica", Capo III "della falsità in atti":

art. 491-bis ("Documenti informatici"): *"Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli."*[8]

Il problema principale è che il documento informatico non viene compreso nella sua vera essenza che lo slega dalla materialità; mentre il documento cartaceo lega indissolubilmente contenuto e

[7] *Dialer, trojan horse: cosa si nasconde dietro un click*, <http://www.giuristitelematici.it/modules/bdnews/article.php?storyid=104>

[8] Da precisare che la normativa distingue tra falsità materiale e falsità ideologica; la prima identifica una non corrispondenza tra autore e testo, la seconda identifica una non veridicità delle dichiarazioni contenute nel documento stesso.

contenente, nel documento informatico tutto ciò non avviene ed è dunque limitativo ricondurlo al "*supporto informatico*".[9]

Detto ciò bisogna quindi chiarire cosa si intende per "documento informatico".

Il documento informatico è sostanzialmente un documento immateriale e dinamico, ed è la "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*" (come definito dal D.P.R. 513/97 art 1 lettera "a" e riconfermato nel D.P.R. 445/2000 art. 1 lettera "b") in quanto non vi è alcuna distinzione tra l'originale e la copia.

Non si tratta dunque di un mero cambio di supporto rispetto al preesistente documento cartaceo, ma di un cambio nella concezione vera e propria di documento che nell'informatica, come detto, assume i caratteri di *rappresentazione*.[10]

Il documento informatico acquista effettiva valenza legale con la legge 59/1997 (art. 15 comma 2).

Per poter però essere valido un documento deve poter essere autenticato e se ne deve poter attribuire la paternità.

A tale scopo interviene la *firma digitale*, e nel D.P.R. 513/97 art. 1 lettera "b" se ne da una definizione: s'intende "*per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*".

Con la firma digitale dunque si attesta anche l'integrità ed il non ripudio del documento (quindi si scongiura la falsità materiale), in quanto nella procedura di firma digitale viene generato un particolare codice crittografico derivante dalla "mescolanza" dei dati identificativi del mittente con

---

[9] *Hacking e criminalità informatica - l'approccio normativo alla criminalità informatica (capitolo III),* op. cit.

[10] *Il falso informatico*,
<http://www.filodiritto.com/diritto/privato/informaticagiuridica/falsoinformaticopetruzzelli.htm>

il contenuto vero e proprio del documento (*hash*); qualora al momento della ricezione vi sia corrispondenza tra i codici crittografici ottenuti, si avrebbe conferma dell'integrità del documento e dell'autenticità del mittente.

Tutto ciò viene confermato dall'art. 5 del suddetto D.P.R. 513/97, in cui si specifica la validità quale scrittura privata del documento informatico sottoscritto con la firma digitale, nonché la sua efficacia probatoria.[11]

Dunque nel caso in cui un documento venga deliberatamente falsificato (sia falsità materiale che ideologica) vengono applicate le pene di cui agli articoli che regolamentano le falsità in atti delle scritture private e degli atti pubblici (Titolo VII , Capo III).

Il Codice Penale regolamenta poi una terza macrocategoria, che riguarda *l'integrità dei dati e dei sistemi informatici*, attraverso vari articoli, tra cui il 635-bis sul "danneggiamento di sistemi informatici e telematici", contenuto nel Titolo XIII "dei delitti contro il patrimonio", Capo I " dei delitti contro il patrimonio mediante violenza alle cose o alle persone";

art. 635-bis ("Danneggiamento di sistemi informatici e telematici"): *"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*

Se ricorre una o più delle circostanze di cui al secondo comma dell'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."

L'art. 635-bis del Codice Penale ripropone il reato di danneggiamento (previsto dall'art. 635 c.p.) in rapporto non solo alle apparecchiature informatiche o telematiche, ma anche ai dati, informazioni

[11] *Falsificazione della firma digitale: un rischio evitabile*, <http://www.diritto.it/materiali/tecnologie/calabrese.html>

o programmi in esse contenute, necessariamente caratterizzati da immaterialità e difficili da punire con il generico reato di danneggiamento.

Nell'ambito dell'art. 635-bis si parla infatti di danneggiamento totale o parziale, di deterioramento e di distruzione. Con la prima espressione si fa riferimento alle modalità attraverso cui si può rendere del tutto o in parte inservibile un sistema informatico/telematico, con la seconda ci si riferisce alla creazione di guasti in grado di far scemare le prestazioni del sistema, mentre nella terza espressione ci si riferisce ad un'azione di annullamento totale di un sistema.

La miglior tecnica preventiva adottabile dall'utenza (privata o aziendale) è quella di dotarsi di efficienti sistemi di *backup*, in grado di sopperire all'eventuale perdita di dati e informazioni.

Aggravante del reato "danneggiamento di sistemi informatici e telematici" è l'art. 420 c.p. "attentato a impianti di pubblica utilità" contenuto nel Titolo V "dei delitti contro l'ordine pubblico";

art. 420 ("Attentato a impianti di pubblica utilità"): *"Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.*

La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti.

Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni."

Si tratta dunque di un'estensione nei reati di danneggiamento a sistemi informatici, che trova qui ora un inasprimento nel caso in cui il reato di danneggiamento sia compiuto contro impianti di pubblica utilità e quindi di pericolo per l'ordine pubblico e per gli interessi socio-economici collettivi.

Il Codice Penale interviene anche estendendo l'art. 392 ai sistemi informatici (comma 3);

art. 392 ("Esercizio arbitrario delle proprie ragioni con violenza sulle cose"): *"Chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice, si fa arbitrariamente ragione da sé medesimo, mediante violenza sulle cose, è punito a querela della persona offesa, con la multa fino a euro 516.*
Agli effetti della legge penale, si ha violenza sulle cose allorché la cosa viene danneggiata o trasformata, o ne è mutata la destinazione.
Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico."

A tal riguardo viene punito colui che ricorre al "regolamento di conti" attraverso l'uso della violenza sulle cose al fine di manifestare un preteso diritto.

Riferito all'informatica si tratta dell'alterazione, modifica o cancellazione in tutto od in parte di un programma al fine di turbarne il corretto funzionamento.[12]

Interessante da analizzare è infine l'art. 615-quinquies, attraverso cui si meglio precisa un aspetto già genericamente affrontato dall'art. 635-bis. Contenuto 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", recita:

art. 615-quinquies ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico"): *"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329."*

Con l'art. 615-quinquies si mira a reprimere la "*diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*", tutti i programmi cioè rientranti sotto la categoria di malicious software (o malware).

[12] S. Nespor, A. De Cesaris, *Internet e la Legge*, Hoepli, 2001, pp. 363-364

Il fatto che vi sia un articolo del Codice Penale unicamente dedicato a questa tipologia di software, evidenzia come la diffusione stessa di questi malware sia molto alta.

Le categorie che rientrano sotto l'etichetta di malware sono molte ma, in linea generale, sono tutte accomunate dal medesimo scopo di danneggiare un sistema informatico (specialmente in riferimento alla sua parte "software").

La categoria di malware più diffusa e conosciuta è quella dei virus, speciali parti di codice che si diffondono copiandosi all'interno di altri programmi, in modo tale da essere eseguiti ogni volta che il file infetto viene aperto. [13]

La diffusione dei virus è legata alla trasmissione di questi file infetti, che può avvenire sia attraverso comuni supporti di memorizzazione magneto-ottica, sia attraverso una distribuzione su reti telematiche. Queste ultime, in special modo Internet, hanno poi dato terreno fertile alla diffusione di altri malicious code, tra cui worm, trojan horse, backdoor e spyware, solo per citare i più comuni.

Attraverso l'art. 615-quinquies si mira dunque a reprimere la diffusione di questi codici maligni (indipendentemente dalla scopo per cui sono creati), e costituisce reato la distribuzione di supporti contenenti malware, o la loro diffusione attraverso reti telematiche (non è pertanto punita la creazione o la semplice detenzione di tali software).

Da precisare però che tale reato è punito solo qualora vi sia dolo e non lo è nel momento in cui si accerti una condotta meramente colposa. Ciò serve a scagionare tutti quegli individui che si vedono vittime ignare ed inconsapevoli della diffusione dei malware (con particolare riferimento agli worm, che si riproducono senza il consenso dell'utente ed a sua insaputa).

---

[13] *Malware*, <http://it.wikipedia.org/wiki/Malware>

Inoltre l'art. 615-quinquies individua un reato di pericolo, in cui non necessariamente si deve verificare una distruzione (parziale o totale), come invece avviene nel caso dell'art. 635-bis (reato di evento).[14]

Dal punto di vista della prevenzione è possibile ricorrere all'utilizzo di software quali *antivirus*, *antispyware*, ecc. che, se opportunamente aggiornati, sono in grado di segnalare all'utente l'eventuale presenza di software maligni.

Ultima macrocategoria dei reati informatici è quella inerente la *riservatezza dei dati e delle comunicazioni informatiche*.

In tale ambito il Codice Penale interviene con l'intento di reprimere forme di intrusione nella sfera privata altrui.

Il primo provvedimento previsto dalla legge 547/93 in materia di riservatezza dei dati e delle comunicazioni informatiche è quello adottato con l'art. 615-ter del Codice Penale

"*accesso abusivo ad un sistema informatico o telematico*", Titolo XII "dei delitti contro la persona", Capo III "dei delitti contro la libertà individuale", Sezione IV "dei delitti contro la inviolabilità del domicilio";

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

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,

[14] *Il delitto di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*, <http://www.computerlaw.it/public/perfetti_615quinquies.pdf>

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 palesamente 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."

Con questo articolo si vuole tutelare il sistema informatico, inteso qui come vera e propria estensione del domicilio dell'individuo, al fine di proteggerlo da accessi non autorizzati e da permanenza non gradita (tutela peraltro garantita dall'art. 14 della Costituzione Italiana[15]).

Ciò che immediatamente si coglie dall'art. 615-ter è che un sistema per poter subire un accesso abusivo, deve essere protetto da una qualsivoglia forma di sicurezza (sia essa una forma di protezione logica – ad esempio nome utente e password - o fisica – vigilantes o porte blindate a protezione dei sistemi informatici; ed è d'altronde questo il caso in cui si può applicare il punto due del secondo comma)[16], e ciò presuppone un palesato interesse dell'individuo a voler tutelare i propri dati (ed in ciò si distingue anche la differenza del domicilio informatico da quello "reale" tutelato dall'art. 614 c.p.; essendo infatti il domicilio informatico un "luogo" estremamente

[15] *La Costituzione della Repubblica Italiana*, <http://www.quirinale.it/costituzione/costituzione.htm>

[16] *Interpretazione dell'articolo 615-ter del Codice Penale*, <http://www.diritto.it/materiali/penale/merola.html>

flessibile ed aperto, non si può tutelare il domicilio a priori in quanto tale, ma si deve tutelare solo ciò che esplicitamente il titolare ha deciso che deve rimanere riservato, e tale volontà esplicita è manifestata attraverso l'adozione di una misura di sicurezza).

Nel caso infatti in cui il sistema informatico non sia protetto in alcun modo non può sussistere il reato di accesso abusivo.

Da precisare inoltre che con l'art. 615-ter non si fa alcun riferimento ad eventuali danni causati dall'accesso abusivo al sistema (questione già affrontata con l'art. 635-bis), ma si mira a reprimere esclusivamente l'atto di accesso ad un sistema per il quale non si hanno i diritti per accedervi o per permanervi oltre la durata stabilita dal titolare del sistema.[17]

Ciò che dunque appare importante alla luce dell'art. 615-ter è la salvaguardia dei dati contenuti all'interno del proprio "domicilio" informatico.

Dal punto di vista della prevenzione appare evidente che tra le possibili soluzioni per scongiurare un accesso abusivo, ci sia quella di regolare l'accesso per selezione (o, di contro, per esclusione).

A tal riguardo una delle più semplici misure da adottare è quella di impostare un *account* dotato di *nome utente* e *password* di accesso. Altra soluzione, più dispendiosa ma anche più efficace, è quella di dotarsi di un *firewall* al fine di controllare gli accessi.[18]

In ogni caso, come già specificato, occorre che sia presente un, seppur minimo, sistema di protezione al fine di poter parlare di accesso abusivo in relazione all'art. 615-ter c.p.[19]

Altre disposizioni del Codice Penale in materia di *riservatezza dei dati e delle comunicazioni informatiche*, le si possono riscontrare nell'art. 615-quater:

---

[17] *I reati informatici nell'ordinamento italiano*, <http://www.oilproject.org/logs/dispense/diritto_penale_reati.pdf>

[18] *Sicurezza informatica*, <http://it.wikipedia.org/wiki/Sicurezza_informatica>

[19] *Sentenza Corte di Cassazione Sez VI, 27 ottobre 2004 (dep. 30 novembre 2004), n. 46509,* <http://www.penale.it/page.asp?mode=1&IDPag=174>

art. 615-quater ("Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici"): *"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino 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."

Anche l'art. 615-quater è compreso (come il 615-ter) 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". A differenza dell'art. 615-ter però, l'art. 615-quater fa riferimento al possesso indebito ed all'eventuale diffusione di codici di accesso e non il loro utilizzo ai fini di un accesso abusivo.

Tale articolo punisce dunque la detenzione non autorizzata di codici di accesso (con codici di accesso si intendono non solo password ma anche P.I.N., smart card criptate o eventuali sistemi biometrici, come le impronte digitali ed il riconoscimento vocale), ma anche la loro diffusione illecita a terzi non autorizzati. Inoltre è contemplato quale reato anche la diffusione di istruzioni tecniche su come eludere od ottenere i suddetti codici di accesso.[20]

In ogni caso non è sufficiente la detenzione o la diffusione di codici illeciti per poter incorrere nelle pene previste dall'articolo in questione, ma è necessario che da tale detenzione o diffusione ne derivi un profitto per sé o per altri o altresì un danno a terzi.

Sempre in riferimento alla macrocategoria sulla *riservatezza dei dati e delle comunicazioni informatiche*, il Codice Penale individua nell'art. 621 (Titolo XII "dei delitti contro la persona",

[20] *Diffusione e detenzione abusiva di codici d'accesso*, <http://www.studioferragina.com/mdb-database/ecrimes/detabucod.PDF>

Sezione V “dei delitti contro la inviolabilità dei segreti”) un ulteriore forma di protezione della riservatezza dei propri documenti;

art. 621 (“Rivelazione del contenuto di documenti segreti”): *“Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da euro 103 a euro 1.032.*
Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.

Il delitto è punibile a querela della persona offesa.”

La legge 547/93 estende l’art. 621 c.p. anche ai documenti informatici, rendendo di fatto punibile come reato la rivelazione del contenuto di documenti riservati e da cui se ne trae un indebito profitto per sé o per altri, oltreché un danno per il titolare dello stesso.

Più nello specifico dell’ambito informatico entrano gli artt. *617-quater*, *617-quinquies e 617-sexies (*Titolo XII “dei delitti contro la persona”, Sezione V “dei delitti contro la inviolabilità dei segreti”), i quali tutelano la riservatezza delle comunicazioni informatiche proprio come nello stesso Codice Penale sono tutelate le comunicazioni per mezzo di apparecchiature telefoniche, telegrafiche ed epistolari attraverso gli artt. 617 e ss. Il fine ultimo di tali articoli è comunque quello espresso attraverso l’art. 616 c.p. sulla “Violazione, sottrazione e soppressione della corrispondenza”, sostenuto, tra l’altro, anche dall’art. 15 della Costituzione Italiana sulla libertà e segretezza della corrispondenza e della comunicazione.

Nello specifico gli artt. 617-quater, 617-quinquies e 617-sexies:

art.617-quater (“Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche”): *“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."

art. 617-quinquies ("Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche"): *"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'articolo 617-quater."

art. 617-sexies ("Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche"): *"Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma

dell'articolo 617-quater."

Gli articoli si riferiscono chiaramente a tutte quelle forme di comunicazione informatica per cui è prevista una identificazione ben precisa dei/del destinatario (es. e-mail, chat dirette ad un utente preciso, ecc), in cui cioè esiste una reale forma di corrispondenza inviolabile, la quale non esiste invece per le forme di comunicazione in cui i destinatari non sono ben definibili e specificati (es. siti pubblici del world wide web, chat pubbliche, ecc.).[21]

A tal proposito viene invece a tutela l'art. 21 della Costituzione Italiana (inerente la libertà di manifestare il proprio pensiero).

Detto ciò appare evidente come il reato di cui all'art. 617-quinquies si disponga in una posizione prodromica rispetto all'art. 617-quater, in quanto il primo si colloca in una fase antecedente l'intercettazione vera e propria e non è necessaria la prova dell'avvenuta intercettazione, interruzione o impedimento della comunicazione, essendo sufficiente accertare l'obiettiva potenzialità lesiva dell'apparecchiatura. Nel caso in cui avvenga poi l'effettiva intercettazione, interruzione o impedimento, si procederà secondo quanto previsto dall'art. 617-quater.

Con l'art. 617-sexies si mira invece a sanzionare l'impiego e la rivelazione pubblica dei contenuti precedentemente intercettati, nonché la loro falsificazione, alterazione o soppressione a scopo di profitto o a danno di altri, condizione necessaria perché sussista il reato.

Da precisare poi, ai fini soprattutto dell'art. 617-quater, che l'intercettazione si verifica nel momento in cui si carpisce, in maniera fraudolenta ed all'insaputa dei soggetti coinvolti nella comunicazione, il contenuto del messaggio trasmesso. Qualora i soggetti coinvolti nella comunicazione autorizzino l'intercettazione il reato non sussisterebbe.[22]

---

[21] *I reati informatici nell'ordinamento italiano*, op. cit.

[22] *La disciplina penale degli illeciti in materia di tecnologie informatiche*, <http://www.trani-ius.it/opinioni/Pica5.html>

In ogni caso, perché si possa parlare di "intercettazione", il messaggio deve giungere integralmente al suo destinatario previsto; in caso in cui il messaggio non giunga al destinatario ma venga interrotto lungo il suo cammino si parlerebbe di "interruzione"; nel caso in cui invece la comunicazione non potesse nemmeno partire si parlerebbe di "impedimento".[23]

Tra le principali tipologie di reati che possono rientrare negli articoli di cui sopra, e specificatamente nell'art. 617-quater, vi è lo *Sniffing*, una tecnica finalizzata a carpire i dati e le informazioni che attraversano una rete telematica.

Dal punto di vista preventivo la miglior soluzione per proteggersi da eventuali intercettazioni di comunicazioni informatiche, operate attraverso attacchi sniffing od altre modalità, è quella di adottare tecniche crittografiche che consentano di rendere illeggibile il contenuto del documento a chi è privo dell'autorità per farlo. La tecnica crittografica più diffusa è attuata attraverso il programma *PGP* (*Pretty Good Privacy*), che consente di rendere sicure le comunicazioni su reti telematiche e non, adottando in special modo la crittografia asimmetrica, peraltro già osservata nell'implementazione della firma digitale.[24]

art. 623-bis ("Altre comunicazioni e conversazioni"): *"Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati."*

Con l'art. 623-bis si vuole semplicemente estendere il campo di riferimento degli articoli sin qui discussi (ed appartenenti alla sezione "dei delitti contro la inviolabilità del domicilio") a qualunque tipo di trasmissione, sia essa, indifferentemente, di dati, suoni o immagini.

---

[23] *Hacking e criminalità informatica - l'approccio normativo alla criminalità informatica (capitolo III),* op. cit.

[24] *Crittografia asimmetrica*, <http://it.wikipedia.org/wiki/Crittografia_asimmetrica>

Con tale precisazione si cerca di entrare in linea con quelli che sono gli sviluppi della multimedialità ed in generale dell'informatica più recente, basata sulla convergenza dei vari media e sulla continua innovazione delle tecnologie di trasmissione.[25]

REGOLAMENTAZIONE COMUNITARIA IN MATERIA DI REATI INFORMATICI

Dalle analisi sui reati informatici previsti dal Codice Penale italiano, appare evidente come ci sia un forte interesse nel disciplinare tali illeciti.

Tali provvedimenti normativi tendono però a perdere la loro efficacia se non correttamente supportati da provvedimenti a livello comunitario.

Il principale problema derivante dalla regolamentazione del crimine informatico deriva infatti dalla sua "aterritorialità".

Si pongono dunque problemi che si collocano a diversi livelli:

1 – a livello investigativo (ampio terreno da monitorare);

2 – a livello processuale (chi è competente a fare cosa);

3 – a livello di diritto penale (a quale legge penale, di quale Stato, bisogna fare riferimento).[26]

Emerge dunque la necessità di dotare l'Unione Europea di una normativa che sappia armonizzare le varie disposizioni nazionali, al fine di rendere più omogeneo ed efficace l'intervento sui computer crimes.

---

[25] *Codice Penale*, <http://www.altalex.com/index.php?idnot=36653>

[26] S. Nespor, A. De Cesaris, *Internet e la Legge*, op. cit., pp. 349-351

E' a partire dal 1997 che si sente l'esigenza di armonizzare concretamente le normative nazionali a livello comunitario, dapprima con la risoluzione sulle "priorità della cooperazione nei settori della giustizia e degli affari interni", in cui si specifica la necessità di combattere il crimine informatico attraverso gli strumenti informatici stessi, poi con il documento definito dal "Gruppo multidisciplinare contro la criminalità organizzata", in cui si prevedono misure e strategie di coordinamento transnazionali.

Nel 1999 si svolge poi a Tampere il primo Consiglio europeo (con 15 Stati membri) interamente dedicato al settore Giustizia e affari interni, e soprattutto ai reati legati all'utilizzo delle tecnologie; a tal riguardo si indica espressamente che l'obiettivo primo è quello di dotarsi di sanzioni comuni.[27]

E' però con la *Convenzione di Budapest sul cyber crime* (firmata il 23 novembre 2001) che si vuole dare una più decisa sferzata alla lotta contro il crimine informatico.[28]

A tal proposito è recente (20 febbraio 2008) l'approvazione, alla Camera dei Deputati, del disegno di legge (proposto in data 19 giugno 2007) di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.[29]

Le principali modifiche al Codice Penale riguardano:

- L'art. 635-bis ("*Danneggiamento di informazioni, dati e programmi informatici*") è stato affiancato dagli artt. 635-ter ("*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*") e 635-quater ("*Danneggiamento di sistemi informatici o telematici*"). Ciò che emerge è una

[27] *L'azione dell'Unione europea nel campo della lotta contro la criminalità ad alta tecnologia*, <http://www.giustizia.it/cassazione/convegni/dic2000/salazar.pdf>

[28] *Convenzione sulla criminalità informatica*, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=3/16/2007&CL=ITA>

[29] *Disegno di legge n. 2807*, <http://www.camera.it/_dati/lavori/stampati/pdf/15PDL0031070.pdf>

chiara distinzione tra il danneggiamento dell'integrità dei dati (art. 635-bis) ed il danneggiamento dell'integrità del sistema (art. 635-quater). Il 635-ter estende il 635-bis ai reati commessi contro lo Stato o enti di pubblica utilità.

- L'art. 491-bis viene aggiornato nella sua definizione di documento informatico, inteso non più come "qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli", bensì come "*rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*", come peraltro già previsto dal D.P.R. 513/97. E' stato inoltre introdotto l'art. 495-bis, inerente la "*Falsa dichiarazione o attestazione al certificatore sull'identità o su qualità personali proprie o di altri*".[30]
- Nell'art. 615-quinquies ("*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*") viene introdotta l'effettiva intenzione di danneggiamento. Ciò è utile a scagionare dal reato penale tutti coloro che si occupano di sicurezza informatica, e che quindi sono spesso portati a compiere danneggiamenti a sistemi terzi al solo scopo di testarne la sicurezza.[31]

In termini di cooperazione comunitaria risulta essere molto importante anche la Decisione Quadro[32] 2005/222/GAI[33] del 24 febbraio 2005, tra gli ultimi atti in materia di reati informatici a livello europeo.[34]

---

[30] *La camera approva la ratifica della convenzione del Consiglio d'Europa sulla criminalità informatica*, <http://www.agatinogrillo.it/content/domani-nella-battaglia-pensa-me-di-javier-marias?q=node/307>

[31] *Convenzione sul cybercrime, ratifica più vicina,* <http://punto-informatico.it/2197407/PI/News/L-Italia-ha-ratificato-la-Convenzione-sul-cybercrime/p.aspx>

[32] La "decisione-quadro" è utilizzata per ravvicinare le disposizioni legislative e regolamentari degli Stati membri. Essa può essere proposta su iniziativa della Commissione o di uno Stato membro e deve essere adottata all'unanimità. Vincola gli Stati membri per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma ed ai mezzi da impiegare a tal fine.

Di sicuro interesse, ed assai esplicativi, risultano essere alcuni dei considerando di tale Decisione Quadro (che si rivolge ai 25 Stati membri):

(1) *L'obiettivo della presente decisione quadro è quello di migliorare la cooperazione tra le autorità giudiziarie e le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione.*

(5) *Le rilevanti lacune e le notevoli differenze nelle normative degli Stati membri in questo settore possono ostacolare la lotta contro la criminalità organizzata ed il terrorismo e complicare un'efficace cooperazione giudiziaria e di polizia nel campo degli attacchi contro i sistemi di informazione. Il carattere transnazionale e senza frontiere dei moderni sistemi di informazione fa sì che gli attacchi contro tali sistemi siano spesso di natura transnazionale, e rende evidente la necessità di adottare urgentemente azioni ulteriori per il ravvicinamento delle legislazioni penali in questo settore.*

(8) *Le legislazioni penali nel settore degli attacchi ai danni di sistemi di informazione dovrebbero essere ravvicinate al fine di garantire la cooperazione giudiziaria e di polizia più ampia possibile nel settore dei reati attinenti agli attacchi ai danni di sistemi di informazione, e di contribuire alla lotta contro la criminalità organizzata ed il terrorismo.*

---

[33] *Decisione Quadro 2005/222/GAI*, <http://europa.eu.int/eur-lex/lex/LexUriServ/site/it/oj/2005/l_069/l_06920050316it00670071.pdf>

[34] *Reati informatici e attività di indagine*, <http://www.convegnovarenna.giuristitelematici.it/relazioni/galdieri.pdf>

Appare dunque evidente come lo scopo principe di questa Decisione Quadro sia quello di armonizzare e rendere effettiva la cooperazione a livello transnazionale al fine di poter combattere il cyber crimine che, per antonomasia, è transfrontaliero e necessita dunque di una normativa più serrata ed efficace.

Per quanto riguarda il corpus effettivo della Decisione Quadro, appare molto interessante il secondo paragrafo dell'art. 8 ("*Responsabilità delle persone giuridiche*"), in cui si sostiene la punibilità penale dell'azienda che non attua una corretta sorveglianza e non applica idonee misure di sicurezza e, da tal superficialità, ne derivi un vantaggio per la stessa.

Altra disposizione prevista dalla Decisione Quadro è quella di cui all'art. 10, in cui si stabilisce la competenza giurisdizionale per ogni Stato membro in caso concorrano uno dei seguenti parametri:

a) il reato è stato commesso interamente o in parte sul suolo dello Stato membro;
b) il reato è stato commesso da un suo cittadino;
c) il reato è stato commesso a beneficio di una persona giuridica che ha sede legale nel territorio dello Stato membro.

Al secondo paragrafo di tale articolo si specifica inoltre, in relazione alla lettera a), che per stabilire la propria competenza giurisdizionale esistono due diversi casi:

1- Il reato è stato compiuto da una persona fisicamente presente sul territorio dello Stato membro, indipendentemente da dove si trovavano i sistemi informatici attaccati;
2- Il reato è stato compiuto ai danni di un sistema informatico residente sul territorio dello Stato membro, indipendentemente dal luogo fisico in cui si trovava l'autore del reato.

Tale specificazione prevista dal secondo paragrafo dell'art. 10, consente di estendere la tutela agli attacchi informatici non solo agli Stati UE ma anche agli Stati extra-UE.[35]

[35] *Nuove responsabilità e sanzioni per le Aziende: i reati informatici riconducibili ad omesso controllo*, <http://www.globaltrust.it/documents/legaldoc/giurisprudenza/commenti/Commmento_Frattallone_decisione_2005_222_GAI.pdf>

CONCLUSIONI

Proprio a partire dalle ultime considerazioni in merito ai provvedimenti a livello comunitario, si evince come la battaglia contro i crimini informatici debba necessariamente passare attraverso una serrata ed armonica collaborazione a livello transnazionale.

Tutti gli sforzi che, in questo campo, vengono compiuti dai singoli Paesi membri dell'Unione a livello nazionale, devono trovare una loro espressione anche a livello comunitario.

A rendere particolarmente importante, quanto complessa, l'armonizzazione a livello comunitario, è certamente la particolare caratteristica di extraterritorialità delle nuove reti telematiche.

I reati compiuti a mezzo informatico, come si è visto, sono spesso slegati dal territorio e dunque diventa particolarmente complesso riuscire a punire il reato senza una normativa comune ed omogenea tra i vari Stati membri.

Benché l'Italia, nel caso specifico, sembra essersi dotata di un buon apparato legislativo nei confronti dei cyber crimes, è comunque doveroso sottolineare che tutti i provvedimenti in questione devono poter essere applicati al di là dei propri confini nazionali, pena un rendere, se non inutili, quanto mai vani tutti gli sforzi posti in essere.

Per ultimo, ma non certo per importanza, è quanto mai importante coltivare, ai fini di una graduale riduzione del crimine informatico ed in parallelo allo sviluppo coordinato delle normative transnazionali, una nuova cultura informatica, che sappia ben informare e sensibilizzare l'utenza sui vantaggi ma anche sui rischi che è possibile correre attraverso un incauto utilizzo delle nuove tecnologie legate all'informatica ed alla telematica.

Dr Mauro Ventura

BIBLIOGRAFIA e SITOGRAFIA

Codice Penale, <http://www.altalex.com/index.php?idnot=36653>

Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, <http://www.giustizia.it/pol_internaz/tutela/ce_salv_diritti.htm>

Convenzione sul cybercrime, ratifica più vicina, <http://punto-informatico.it/2197407/PI/News/L-Italia-ha-ratificato-la-Convenzione-sul-cybercrime/p.aspx>

Convenzione sulla criminalità informatica, <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=3/16/2007&CL=ITA>

Crittografia asimmetrica, <http://it.wikipedia.org/wiki/Crittografia_asimmetrica>

Decisione Quadro 2005/222/GAI, <http://europa.eu.int/eur-lex/lex/LexUriServ/site/it/oj/2005/l_069/l_06920050316it00670071.pdf>

Dialer, trojan horse: cosa si nasconde dietro un click, <http://www.giuristitelematici.it/modules/bdnews/article.php?storyid=104>

Diffusione e detenzione abusiva di codici d'accesso, <http://www.studioferragina.com/mdb-database/ecrimes/detabucod.PDF>

Direttiva 2006/24/CE, <http://www.garanteprivacy.it/garante/document?ID=1485189>

Disegno di legge n. 2807, <http://www.camera.it/_dati/lavori/stampati/pdf/15PDL0031070.pdf>

Falsificazione della firma digitale: un rischio evitabile, <http://www.diritto.it/materiali/tecnologie/calabrese.html>

Hacking e criminalità informatica - l'approccio normativo alla criminalità informatica (capitolo III), <http://www.altrodiritto.unifi.it/devianza/tavassi/nav.htm?cap3.htm>

I reati informatici nell'ordinamento italiano, <http://www.oilproject.org/logs/dispense/diritto_penale_reati.pdf>

Il delitto di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, <http://www.computerlaw.it/public/perfetti_615quinquies.pdf>

Il falso informatico, <http://www.filodiritto.com/diritto/privato/informaticagiuridica/falsoinformaticopetruzzelli.htm>

Il phishing: analisi, dati e previsioni, <http://www.jei.it/approfondimentigiuridici/notizia.php?ID_articoli=545>

S. Nespor, A. De Cesaris, *Internet e la Legge*, Hoepli, 2001

Interpretazione dell'articolo 615-ter del Codice Penale,
<http://www.diritto.it/materiali/penale/merola.html>

L'azione dell'Unione europea nel campo della lotta contro la criminalità ad alta tecnologia,
<http://www.giustizia.it/cassazione/convegni/dic2000/salazar.pdf>

La camera approva la ratifica della convenzione del Consiglio d'Europa sulla criminalità informatica, <http://www.agatinogrillo.it/content/domani-nella-battaglia-pensa-me-di-javier-marias?q=node/307>

La Costituzione della Repubblica Italiana, <http://www.quirinale.it/costituzione/costituzione.htm>

La disciplina penale degli illeciti in materia di tecnologie informatiche,
<http://www.trani-ius.it/opinioni/Pica5.html>

Malware, <http://it.wikipedia.org/wiki/Malware>

Nuove responsabilità e sanzioni per le Aziende: i reati informatici riconducibili ad omesso controllo,
<http://www.globaltrust.it/documents/legaldoc/giurisprudenza/commenti/Commmento_Frattallone_decisione_2005_222_GAI.pdf>

Nuove tecnologie Nuove criminalità,
<http://www.reportonline.it/modules.php?name=News&file=print&sid=2122>

OCSE, *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione*,
<http://www.oecd.org/dataoecd/16/23/15582268.pdf>

Reati informatici e attività di indagine,
<http://www.convegnovarenna.giuristitelematici.it/relazioni/galdieri.pdf>

Sentenza Corte di Cassazione Sez VI, 27 ottobre 2004 (dep. 30 novembre 2004), n. 46509,
<http://www.penale.it/page.asp?mode=1&IDPag=174>

Sicurezza informatica, <http://it.wikipedia.org/wiki/Sicurezza_informatica>