I REATI INFORMATICI

INTRODUZIONE ALLA PROBLEMATICA

I REATI INFORMATICI, O *COMPUTER CRIMES: RISVOLTO NEGATIVO DELLO* SVILUPPO TECNOLOGICO.

- 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.

DALCONNUBIOINFORMATICA-RETI TELEMATICHE ORIGINANO AMPIE POSSIBILITÀ PER LA CRESCITA DELLA SOCIETÀ.

- 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.

IDONEE CONTROMISURE

- 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.

Prevenzione e repressione

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

- 1: **Prevenzione dei reati (lato utente e lato pubblica sicurezza)**
- 2- **Repressione dei reati (Codice Penale e disposizioni comunitarie)**

SENSIBILIZZAZIONE DELL'UTENTE

- 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 crime2, 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.

PUBBLICA SICUREZZA

- 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).

LEGGE 547/93

- La prima vera normativa contro i 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*").

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.*

1 MACROCATEGORIA: 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.**
- **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."**

PHISHING

- Tra i reati che più frequentemente vengono compiuti, e che ricadono, tra gli altri, all'interno della "frode informatica", vi sono le cd. pratiche di ***Phishing*** *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.

ISTRUZIONI E CONSIGLI (1)

- **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 email 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;**
- **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 @;**

ISTRUZIONI E CONSIGLI (2)

- **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.**

DIALER.

- 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.
- 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.

- Innanzitutto è possibile disabilitare presso il proprio operatore telefonico le chiamate verso numerazioni internazionali e/o verso i numeri speciali a pagamento.
- Altro provvedimento che è possibile adottare è quello di utilizzare una linea telefonica basata su tecnologia ADSL od a fibra ottica che, effettuando chiamate dirette e verso un solo numero, non subisce alcun danno dai dialer

SECONDA MACROCATEGORIA: FALSIFICAZIONI

- 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."***

DOCUMENTO INFORMATICO

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

- 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.*

ART. 24 - FIRMA DIGITALE EX 235/2010

Art. 24 - Firma digitale

- 1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

- 2. L'apposizione di firma digita le integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

- 3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

- 4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Falsità in atti

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).

Ma si può falsificare una firma digitale?

TERZA MACROCATEGORIA: INTEGRITÀ DEI DATI…

- *Il codice penale regolamenta 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"

DANNEGGIAMENTO DI SISTEMI INFORMATICI…

- **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."**

DANNEGGIAMENTO, DETERIORAMENTO E DISTRUZIONE

- 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.
- (dotarsi di efficienti sistemi di *backup, in grado di sopperire all'eventuale perdita di dati e informazioni)*

ATTENTATO A IMPIANTI DI PUBBLICA UTILITÀ

- 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."**

VIOLENZA SULLE COSE

- 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.**

DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE….

- **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).

COLPA E VITTIME

- 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).

- 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.

Malware

Nella sicurezza informatica il termine malware indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno.

- I virus, alla fine di numerosi studi hanno "subito" una catalogazione, questa:

VIRUS

- 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.
- 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.

- Un virus informatico non è altro che un programma come gli altri capace di replicarsi tramite "portatori sani" (ovvero file non infetti) e danneggiare (in modi diversi) il sistema.

WORM

- Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

TROJAN HORSE

- Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.

BACKDOOR

- Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

SPYWARE

- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.

DIALER

- Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

HIJACKER

- Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.

ROOTKIT

- Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare spyware e trojan

SCAREWARE

- Scareware: sono così chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, chiamati in gergo rogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta spacciati anche a pagamento.

Rabbit

- Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.

ADWARE

- Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

Batch

- Batch: i Batch sono i cosiddetti "virus amatoriali". Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altre cose dannose) dell'utente a cui viene mandato il file. Non si apre automaticamente, deve essere l'utente ad aprirlo, perciò dato che l'antivirus non rileva i file Batch come pericolosi è sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolosità. Bisogna però anche dire che esistono modi per camuffare i Batch e farli sembrare dei file exe, aumentandone anche il peso per sedare ogni sospetto. L'utilizzo di questo particolare "malware" è spesso ricorrente nel Cyberbullismo.

KEYLOGGER

- I Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i keylogger vengono installati sul computer dai trojan o dai worm, in altri casi invece il keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente.

ROGUE ANTISPYWARE

- Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma

Bomba logica e Zip Bomb

- Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.
- Zip Bomb è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a diventare un file di circa quattro Petabyte, (Peta è un prefisso, SI che esprime il fattore 1015, ovvero 10005, ovvero 1 000 000 000 000 000, ovvero un milione di miliardi.) occupando quindi tutto lo spazio su disco rigido.

QUARTA MACROCATEGORIA: *RISERVATEZZA DEI DATI ….*

- 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,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;**

ART. 615-TER

- **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."**

TUTELA DEL DOMICILIO

- 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 Italiana15).

MISURE DI SICUREZZA

- 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)

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

- 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.*

Altre disposizioni del Codice Penale

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

DIFFUSIONE DI CODICI DI ACCESSO

- 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.

- 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.

RIVELAZIONE DEL CONTENUTO DI DOCUMENTI SEGRETI

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

RISERVATEZZA DELLE COMUNICAZIONI INFORMATICHE

- 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.

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.**

ART. 617-QUATER

- **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

- **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. 17-SEXIES

- **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.”**

E-MAIL, CHAT DIRETTE

- 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.).

RAPPORTO ARTT. 617-QUINQUIES/617-QUATER

- 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.

ART. 617-SEXIES

- 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.

INTERCETTAZIONE E INTERRUZIONE

- 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".

SNIFFING

- 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.

ALTRE COMUNICAZIONI E CONVERSAZIONI

- **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.

CONVENZIONE DI BUDAPEST

- 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.

- 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* 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.**

CONVENZIONE DI BUDAPEST

- 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".*

CONVENZIONE DI BUDAPEST

- 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.

DECISIONE QUADRO32 2005/222/GAI33 DEL 24 FEBBRAIO 2005

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 28 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.*

DECISIONE QUADRO32 2005/222/GAI33 DEL 24 FEBBRAIO 2005

- *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*

DECISIONE QUADRO32 2005/222/GAI33 DEL 24 FEBBRAIO 2005

- *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.*

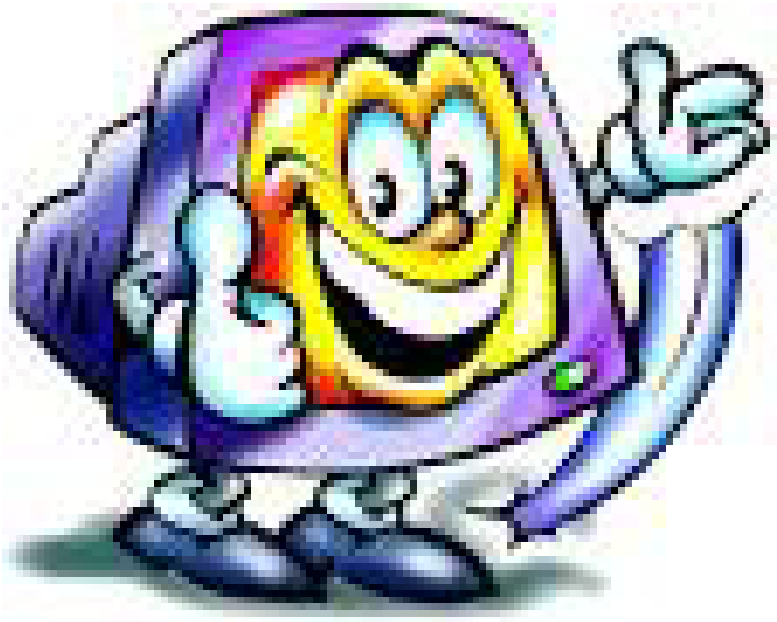
DECISIONE QUADRO32 2005/222/GAI33 DEL 24 FEBBRAIO 2005

- 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.

DECISIONE QUADRO32 2005/222/GAI33 DEL 24 FEBBRAIO 2005

- 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.

Reati informatici



Fine