

Studio Legale Avv. Prof. Cesare Triberti

POLITECNICO DI MILANO

- ***"Digital forensics: un terreno di incontro tra diritto e informatica"***

DIPARTIMENTO ELETTRONICA E
INFORMAZIONE

Sala Seminari, 19 maggio 2008

- **Normativa europea di riferimento:**
- Consiglio UE 28.11.1996
- Risoluzione del Parlamento 27-29.10.1997
- Piano di Azione di Amsterdam giugno 1997
- Riunione del Consiglio a Tampère (FL) 1999
- Direttiva CEE 2000/31 – D.Lgs.70/2003 commercio elettronico
- Raccomandazione 7.9.1999 n.3
- Direttiva CE del Parlamento e Consiglio 12.7.2002 n.58
- Decisione Quadro del Cons. 24.4.2005 . 222
- Direttiva CEE 15.3.2006 n. 24



- **Convenzione di Budapest**
23.11.2001 “
Cybercriminalità”:
 - Obbligo di punizione della complicità
 - Obblighi di collaborazione in capo al Provider ratificata con **L.18.3.2008 n.48**

La Convenzione però, implica solo l'adeguamento degli ordinamenti degli Stati membri, con gli strumenti giuridici più adeguati.

Va tenuto altresì conto che si è proposto di far aderire anche Stati non Cee:
U.S.A., Canada, Australia, Giappone.



- Su tali difficoltà di adeguamento normativo extra Cee, si veda la **Sentenza della Corte di Giustizia CEE 30.5.2006** che ha annullato le decisioni della Commissione e del Consiglio con le quali si era autorizzata la schedatura dei passeggeri degli aerei diretti/provenienti o in transito dagli U.S.A. in quanto ritenute lesive della Privacy.



- Interessante è la **Decisione Quadro 2005/222** relativa agli attacchi contro i sistemi di informazione.
- Si chiede agli Stati di incriminare tre tipologie di condotte:
 - accesso illecito ai sistemi di informazione (art.2)
 - Interferenza illecita sui sistemi (art.3)
 - Interferenza illecita sui dati, comprese le forme di istigazione, favoreggiamento, complicità e tentativo (artt.4-5)

Non vi è obbligo di penalizzazione quando le condotte siano di scarsa gravità



- In realtà in Italia si era già provveduto: con l'introduzione di due precise disposizioni legislative: la **L. 518/92 sulla tutela del software** e la **L. 547/93 sulla criminalità informatica**, si sono portati elementi di indiscutibile rilevanza.
- Precedentemente, l'assenza di una precisa norma penale impediva l'applicazione di sanzioni per fattispecie criminose non codificate.
- Infatti, contrariamente al codice civile che riconosce il principio del ricorso per analogia, l'art. 1 c.p. recita: "Nessuno può essere punito per un fatto che non sia espressamente preveduto come reato dalla legge, né con pene che non siano da essa stabilite."



- In assenza di un dettato normativo nazionale, apparso come visto solo nel 1993, ritenevamo che tutte le classificazioni, pur imperfette, dei reati informatici, dovessero necessariamente tener conto di quanto sviluppato dagli esperti della sicurezza tecnica e dell'audit informatico negli USA ed in altre Nazioni all'avanguardia nel settore , e su tale base parliamo di:
- 1 - *Danneggiamento*: intendendosi con tale termine le azioni criminose attuate:
 - *a) contro :*
 - *hardware*
 - *contro software*
 - *contro il complesso dei mezzi di comunicazione*
 - *b) tramite l'alterazione di dati in modo da produrre un danno all'utilizzatore o a terzi*
- Le due categorie potevano, a loro volta, compenetrarsi vicendevolmente e non escludersi, aggravando così la situazione del soggetto leso.
- Le modalità concrete di attuazione del danneggiamento potevano essere le più svariate , tra cui le rotture volontarie, le esplosioni, il calore, il freddo e così via.



- 2. Vi erano poi le *alterazioni di informazioni* atte ad impedire l'esatto uso di nastri, dischi o programmi e particolarmente:
 - il Superzapping
 - il Data Dilling
 - il Trojan horse
 - l' Anasynchronous attack
 - la Logic Bomb
- 3) Virus
- Una menzione a parte veniva dedicata ai così detti *virus informatici*, che oggi argomento notissimo, alla fine degli anni ottanta apparivano prepotentemente all'attenzione degli utenti e degli operatori informatici.
- Il termine "Virus" venne mutuato dal linguaggio medico per la particolare assonanza del fatto informatico con la capacità di propagazione delle malattie virali ed il paragone si mostrava quanto mai calzante stante la capacità di diffondersi di ciascun virus informatico e la sua spiccata tendenza a invadere sempre nuovi spazi.
- D'altronde il Virus Informatico altro non è che un vero e proprio programma in grado di intaccare altri programmi così come nella realtà medica i virus infettano via via più soggetti man mano che questi ne vengano in contatto.



- Distinguevamo inoltre i Virus Informatici in due primi grandi gruppi:
- *a) Virus maligni o letali*
- *b) Virus benigni o non letali*
- essendo i primi caratterizzati da un elevato livello di pericolosità in quanto inducenti danni irreversibili o comunque difficilmente o difficoltosamente rimediabili, ed i secondi caratterizzati invece da un elevato livello di fastidio .
- Pertanto i Virus Informatici sono caratterizzati da u comportamento tale da dar luogo a molteplici situazioni, quali, ad esempio, la cancellazione di precisi programmi, la creazione di "bad rectors", l'assorbimento di memoria, la formattazione, l'impedimento di operatività del sistema.



- **Art. 615 ter c.p. 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 e' della reclusione **da uno a cinque anni:**

1) se il fatto e' 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 qualita' di operatore del sistema;

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

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

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

Nel caso previsto dal primo comma il delitto e' punibile a querela della persona offesa; negli altri casi si procede d'ufficio (1).

(1)Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.



- **Art. 615 quater c.p. 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 5.164 euro. La pena è della **reclusione da uno a due anni** e della multa da 5.164 euro a 10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater (1).
- *(1) Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547.*



- **Art. 615 quinquies c.p.** Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
- Chiunque allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione totale o parziale, o l'alterazione di suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino ad euro 10.329.
- *(1) Articolo aggiunto dall'art. 4, L. 23 dicembre 1993, n. 547 e modificato dalla L. 18.3.2008 n.48*



- L'art. 615 così formulato offre un innovativo aiuto alla difesa contro uno dei comportamenti illegittimi e maggiormente diffusi del mondo delle comunicazioni informatiche:

Hackeraggio

Nonché offre tutela nei confronti di chi mette in circolazione un **programma** informatico, proprio o di terzi, **idoneo al danneggiamento** di un sistema informatico o telematico, dati o programmi compresi o ad esso pertinenti, o idoneo a creare interruzione totale o parziale del sistema o la sua alterazione.

The word "VIRUS" is rendered in a bold, 3D, light blue font with a dark blue outline. The letters are slightly slanted and have a perspective effect, giving them a three-dimensional appearance. The word is positioned at the bottom center of the slide.

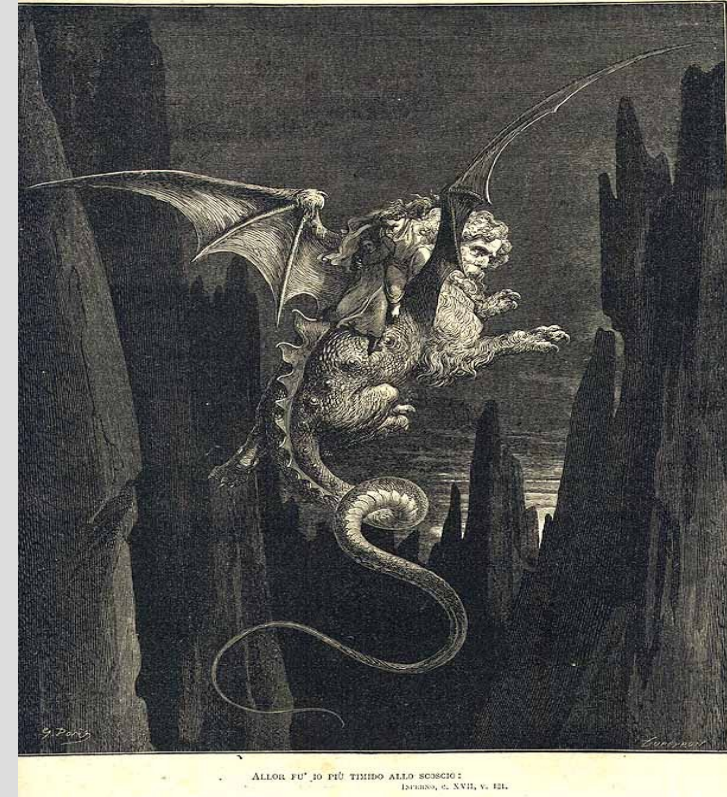
- **Art. 617 quater c.p.** Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche
- Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra piu' sistemi, ovvero le impedisce o le interrompe, e' punito con la **reclusione da sei mesi a quattro anni**.
Salvo che il fatto costituisca piu' 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 e' della **reclusione da uno a cinque anni** se il fatto e' 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 necessita';
 - 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 qualita' di operatore del sistema;
 - 3) da chi esercita anche abusivamente la professione di investigatore privato (1).

(1) Articolo aggiunto dall'art. 6, L. 23 dicembre 1993, n. 547.



- **Art. 640 ter c.p. 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 se' o ad altri un ingiusto profitto con altrui danno, e' punito con la **reclusione da sei mesi a tre anni** e con la multa da 51 euro a 1.032 euro.
La pena e' della **reclusione da uno a cinque anni** e della multa da 309 euro a 1.549 euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto e' commesso con abuso della qualita' di operatore del sistema.
Il delitto e' punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante (1).

- (1) *Articolo aggiunto dall'art. 10, L. 23 dicembre 1993, n. 547*



- **Linee guida del Garante Privacy (1.3.2007) “ Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati...e la disciplina della protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente”**



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

- **Cass. 16.9.1997 n.9211** “ *ai fini dell’operatività del divieto di utilizzo delle apparecchiature per il controllo a distanza dei lavoratori previsto dall’art. 4 L.300/70 è necessario che il controllo riguardi (direttamente o indirettamente) l’attività lavorativa, mentre devono considerarsi fuori da tale ambito i controlli diretti ad accertare condotte illecite del lavoratore (i c.d. **controlli difensivi**), quali ad esempio, i sistemi di controllo dell’accesso ad aree riservate o gli apparecchi di rilevazione di telefonate ingiustificate”*



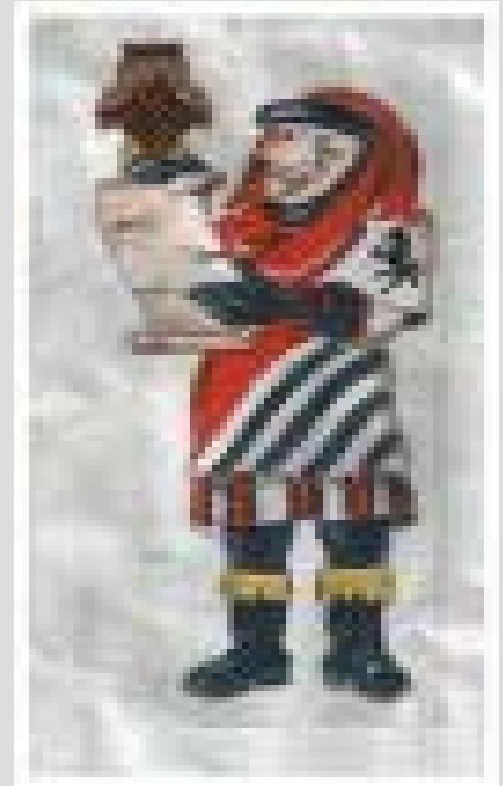
- **Trib. Milano 1.6.2001** ha ritenuto **illegittimo** il collegamento quotidiano per più ore a internet di un dipendente in assenza di effettive necessità lavorative, con conseguente rilevante inadempimento agli obblighi di diligenza, integrando così una giusta causa di licenziamento.
- **Corte App. Milano 30.9.2005** ha ritenuto **illeggittimo** per violazione art. 4 St.L. a seguito di rilevamento con un programma di controllo informatico, del reiterato collegamento a internet in quanto l'uso di quel programma non era stato concordato con accordo sindacale.



- **Cass. Sez. V Penale 19.12.2007 n. 47096.** E' **legittima** la condotta del datore di lavoro che, previa utilizzazione della password, prenda cognizione della corrispondenza informatica contenuta nella casella di posta elettronica del dipendente giacchè non è assimilabile alla corrispondenza *chiusa* e, in quanto tale segreta, quella contenuta in un sistema informatico alla cui utilizzazione siano legittimati anche altri soggetti in quanto aventi sin dall'origine un titolo di accesso (password) da parte del dipendente al superiore gerarchico legittimato ad utilizzarla per accedere al computer anche per la mera assenza dell'utilizzatore abituale.



- **Linee guida del Garante:** paiono complesse e disomogenee: i datori di lavoro devono indicare le modalità d'uso degli strumenti elettronici messi a disposizione e in che misura e con quali modalità vengono effettuati i controlli.
- E a tal fine detta **specifiche linee guida a garanzia** del lavoratore: adozione di un disciplinare interno, di varie misure di tipo organizzativo (impatto sui diritti dei lavoratori, individuazione a chi sia autorizzato l'uso delle mail e di internet, identificazione delle postazioni di lavoro per evitare utilizzi abusivi



- **Rispetto alla navigazione in Internet:**
individuare siti correlati o non correlati alla prestazione lavorativa, configurazione di sistemi o uso di filtri preventivi, trattamento dati in forma anonima, conservazione dei dati per il tempo strettamente necessario alle finalità, graduazione di controlli



- **Utilizzo della posta elettronica:** disposizione di indirizzi condivisi fra più lavoratori, eventualmente affiancandoli a quelli individuali; eventuale attribuzione di un indirizzo ad uso privato; sistemi di invio automatico, in caso di assenze programmate, vari messaggi; delega ad altro lavoratore per accesso in casi giustificati (assenza programmata, malattia, emergenze) , eventuale avvertimento ai destinatari con indicazione della natura non personale e che le risposte potranno essere conosciute dall'organizzazione di appartenenza dell'emittente.



Studio Legale Avv. Prof. Cesare Triberti

Viale Montenero, 51
20135 Milano
Tel. +39-025464737 - 025468217
Fax +39-0255015543
e – mail cesaretriberti@studiolegaletriberti.com
info@studiolegaletriberti.com
www.studiolegaletriberti.com