

# **I reati informatici nell'ordinamento giuridico italiano**

**Avv. Mario Ianulardo**

Università degli Studi di Salerno  
PENETRATION TESTING AND ETHICAL HACKING  
14 marzo 2019

## ***DEFINIZIONE DI SISTEMA INFORMATICO***

*«qualsiasi apparecchiatura o gruppi di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati...» \**

\*art. 1 lett. a) Convenzione di Budapest (2001)

## ***DEFINIZIONE DI DATI INFORMATICI***

*«qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione»*

\*art. 1 lett. b) Convenzione di Budapest (2001)

***"Oggi quasi tutto si svolge sulla Rete"***

***Internet incoraggia un comportamento  
antinormativo, aggressivo, disinibito...***

#### **CONSEGUENZE**

- aumento numero reati c.d. tradizionali commessi con il supporto della tecnologia
- aumento numero reati c.d. informatici

***"Internet incoraggia un comportamento antinormativo, aggressivo, disinibito ...".***

### **CONSEGUENZE**

- necessità applicazione best practice
- necessità di interventi legislativi sottesi a disciplinare nuove ipotesi di reato
- aumento ricorso a prove c.d. digitali

# **CYBER CRIME**

## **interventi legislativi**

### **Legge n. 547/1993**

“Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica”

**Legge n. 155/2005** - contrasto al terrorismo

**Legge n. 38/2006** - contrasto sfruttamento sessuale  
dei bambini e la pedopornografia anche a mezzo Internet

**Legge n. 231/2007** - contrasto ad attività di riciclaggio

# **Legge n. 48/2008**

ratifica ed esecuzione Convenzione Consiglio  
d'Europa (Budapest 2001)\* sulla criminalità  
informatica e norme di adeguamento  
dell'ordinamento interno

- **\*Convenzione di Budapest** 23 novembre 2001



## **Legge n. 38/2009**

in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori (stalking)

## **Legge n. 172/2012**

attuazione della Convenzione del Consiglio d'Europa (Lanzarote 2007) in materia di protezione dei minori dallo sfruttamento e dagli abusi sessuali

## **normativa reati informatici**

**L. 3.5.1991 n. 143** conv. in L. 5.7.1991 n. 197 (art. 12)  
“indebito utilizzo di carte di credito, di pagamento e di documenti che abilitano  
al prelievo di denaro”

**D.Lgs 30.6.2003 n. 196** “protezione dei dati personali”

**D.L.vo 9.4.2003 n. 68**, “diritto di autore” (L. n.633/1941)

**Dlgs 70/2003** attuazione della direttiva 31/2000 CE sul commercio elettronico (artt. 16 e 17) e responsabilità, penale e civile, dei provider

**D.lgs. N. 231/2001** sulla responsabilità degli enti, società ed associazione anche prive di personalità giuridica

# **REATI INFORMATICI**

## **in senso lato**

**diffamazione** (art. 595 c.p.)  
*via internet, SN, forum, chat, etc.*

**ingiuria** (art. 594 c.p.)  
*via email, sms, chat privata*

**favoreggiamento personale** (art. 378 c.p.)  
*es. cancellazione dalla memoria del computer di tracce di un reato commesso da altri*

**associazione a delinquere** (art. 416 c.p.)  
*finalizzata alla commissione di reati informatici*

**falsificazione di un documento** (artt. 476 e 491 bis c.p.)  
*con mezzi informatici*

# **REATI INFORMATICI**

*in senso lato*

## **Violazione diritti d'autore**

*duplicazione abusiva di software (art. 171 bis L. 633/1941)*

**truffa** (art. 648 c.p.)

**estorsione** (art. 629 c.p.)

**ricettazione** (art. 648 c.p.)

**riciclaggio** (art. 648 bis c.p.)

# **REATI INFORMATICI**

*in senso lato*

**sostituzione di persona** (art. 494 c.p.)

**stalking** (art. 612 bis c.p.)

**esercizio arbitrario delle proprie ragioni con violenza sulle cose** (art. 392 c.p.)

**attentato a impianti di pubblica utilità** (art. 420 c.p.)

# **Pedopornografia**

## **Pornografia minorile** (art. 600-ter c.p.)

*pene (da 6 a 12 anni di reclusione) per chi utilizza minori, realizza, produce ... induce minori a partecipare a esibizioni pedopornografiche; commercia, distribuisce, divulga, pubblicizza; offre, cede anche gratuitamente materiale pedopornografico...*

## **Detenzione di materiale pornografico**

(art. 600-quater c.p.)

*(pene fino a 3 anni reclusione)*

## **Pornografia virtuale** (art. 600-quater 1 c.p.)

## **Nuovi reati a sfondo sessuale**

**Istigazione a pratiche di pedofilia e di pedopornografia** (art. 414-bis c.p.)

**Adescamento di minorenni**  
(art. 609-undecies c.p.)

\*introdotti L. n.172/2012

## **Istigazione a pratiche di pedofilia e di pedopornografia (art. 414-bis c.p.)**

*«Salvo che il fatto costituisca più grave reato, chiunque, con qualsiasi mezzo e con qualsiasi forma di espressione, pubblicamente istiga a commettere, in danno di minorenni, uno o più delitti previsti dagli articoli 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater e 609-quinquies è punito con la reclusione da un anno e sei mesi a cinque anni.*

*Alla stessa pena soggiace anche chi pubblicamente fa l'apologia di uno o più delitti previsti dal primo comma. Non possono essere invocate, a propria scusa, ragioni o finalità di carattere artistico, letterario, storico o di costume».*



# **Adescamento di minorenni**

(art. 609-undecies c.p.)

*«Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600 bis, 600 ter e 600 quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600 quinquies, 609 bis, 609 quater, 609 quinquies e 609 octies, adesca un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni.*

*Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione».*

# REATI INFORMATICI

*in senso stretto*

## **Documenti informatici** (art. 491-bis c.p.)

*«Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici».*

*\*«**documento elettronico**», qualsiasi **contenuto conservato in forma elettronica**, in particolare testo o registrazione sonora, visiva o audiovisiva...\**

\*Definizione documento informatico Regolamento EIDAS (910/2014 UE)

# REATI INFORMATICI

*in senso stretto*

**Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri (art. 495-bis c.p.)**

*\*A un documento elettronico non sono negati gli **effetti giuridici** e l'**ammissibilità come prova in procedimenti giudiziari** per il solo motivo della sua forma elettronica.*

\*Definizione art. 46 Regolamento EIDAS (910/2014 UE)

**Accesso abusivo  
a un sistema informatico o telematico  
(art. 615-ter c.p.)**

*«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»*

# **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici** (art.615-quater c.p.)

*«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».*

**Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico  
(art. 615-quinquies c.p.)**

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

# **Violazione, sottrazione e soppressione di corrispondenza**

(art. 616 c.p.)

*...per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, **informatica o telematica**, ovvero effettuata con ogni altra forma di comunicazione a distanza...*

**Intercettazione, impedimento o interruzione illecita  
di comunicazioni informatiche o telematiche**

(art. 617-quater c.p.)

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

(art. 617-quinquies c.p.)



**Falsificazione, alterazione o soppressione del  
contenuto di comunicazioni informatiche o  
telematiche**

(art. 617-sexies c.p.)

**Altre comunicazioni e conversazioni**

(art. 623-bis c.p.)

# **Danneggiamento di informazioni, dati e programmi informatici**

(art. 635-bis c.p.)

*Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.*

*Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.*

# **Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità**

(art. 635-ter c.p.)

*Salvo che il fatto costituisca piu' grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.*

*Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.*

# Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)

*«Salvo che il fatto costituisca più grave reato,  
chiunque **distrugge, deteriora, cancella, altera o  
sopprime** informazioni, dati o programmi informatici  
altrui è punito, a querela della persona offesa, con la  
reclusione da sei mesi a tre anni.*

*Se il fatto è commesso con violenza alla persona o con  
minaccia ovvero con abuso della qualità di operatore del  
sistema, la pena è della reclusione da uno a quattro anni».*

## Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)

# **Frode informatica**

(art. 640-ter c.p.)

*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 51 euro a 1.032 euro.*

## **Frode informatica** (art. 640-ter c.p.)

*La pena è 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 è commesso con abuso della qualità di operatore del sistema.*

*La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*

**Frode informatica del soggetto che presta servizi di  
certificazione di firma elettronica)**  
(art. 640-quinquies c.p.)

**DIGITAL EVIDENCE**

**nel**

**PROCESSO PENALE**

***"Internet incoraggia un comportamento antinormativo, aggressivo, disinibito ...".***

## **CONSEGUENZE**

- necessità applicazione best practice
- necessità di interventi legislativi sottesi a disciplinare nuove ipotesi di reato
- **aumento ricorso a prove c.d. digitali**



# Diritto alla prova

(Art. 190 c.p.p.)

*«Le prove sono ammesse a richiesta di parte.*

*Il giudice provvede senza ritardo con ordinanza escludendo le prove vietate dalla legge e quelle che manifestamente sono superflue o irrilevanti».*

## **Prove non disciplinate dalla legge**

(art. 189 c.p.p.)

*«Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona».*

*(omissis)*

# **La prova digitale da parte della difesa**

## **“Attività investigativa del difensore”**

Art. 327 bis c.p.p.

## **“Investigazioni difensive”**

artt. 391 bis - 391 decies c.p.p.

## **Nomina consulenti tecnici**

(art. 359 c.p.p.)

*Il pubblico ministero, quando procede ad accertamenti, rilievi segnaletici, descrittivi o fotografici e ad ogni altra operazione tecnica per cui sono necessarie specifiche competenze, può nominare e avvalersi di consulenti, che non possono rifiutare la loro opera.*

*Il consulente può essere autorizzato dal pubblico ministero ad assistere a singoli atti di indagine.*

## **Accertamenti tecnici non ripetibili**

(art. 360 c.p.p.)

*Quando gli accertamenti previsti dall'articolo 359 riguardano persone, cose o luoghi il cui stato è soggetto a modificazione, il pubblico ministero avvisa, senza ritardo, la persona sottoposta alle indagini, la persona offesa dal reato e i difensori del giorno, dell'ora e del luogo fissati per il conferimento dell'incarico e della facoltà di nominare consulenti tecnici.*

*2. Si applicano le disposizioni dell'articolo 364 comma 2.*

*3. I difensori nonché i consulenti tecnici eventualmente nominati hanno diritto di assistere al conferimento dell'incarico, di partecipare agli accertamenti e di formulare osservazioni e riserve.*

*4. Qualora, prima del conferimento dell'incarico, la persona sottoposta alle indagini formuli riserva di promuovere incidente probatorio, il pubblico ministero dispone che non si proceda agli accertamenti salvo che questi, se differiti, non possano più essere utilmente compiuti.*

*5. Se il pubblico ministero, malgrado l'espressa riserva formulata dalla persona sottoposta alle indagini e pur non sussistendo le condizioni indicate nell'ultima parte del comma 4, ha ugualmente disposto di procedere agli accertamenti, i relativi risultati non possono essere utilizzati nel dibattimento.*

## **Oggetto della perizia**

(art. 220 c.p.p.)

*«La perizia è ammessa quando occorre svolgere indagini o acquisire dati o valutazioni che richiedono specifiche competenze tecniche, scientifiche o artistiche". (omissis)*

## **Nomina del perito**

(art. 221 c.p.p.)

*«Il giudice nomina il perito scegliendolo tra gli iscritti negli appositi albi o tra persone fornite di particolare competenza nella specifica disciplina. Quando la perizia è dichiarata nulla, il giudice cura, ove possibile, che il nuovo incarico sia affidato ad altro perito". (omissis)*

# **Problema valutazione prove digitali**

- Caratteristiche peculiari digital evidence (immaterialità, ubiquità, indistinguibilità...)
- Problemi di acquisizione, repertamento, conservazione, analisi, etc. (necessità di avvalersi di consulenti tecnici qualificati)
- Digital forensics: scienza recente e non comparativa



# **Falso alibi informatico**

Nel caso di automatismo:  
analisi batteri, DNA, etc ...

**Giudice “peritus peritorum”**

ha il compito di emettere una sentenza giusta e con  
grado di certezza “oltre ogni ragionevole dubbio”

# Determinante il ruolo:

- **C.T.** impegnati a reperire e analizzare digital evidence

**P.G. e Criminologi** per identificare il profilo dell'agente

- **Parti processuali** per accertare la verità dei fatti

**Giurisprudenza** prodotta da Giudici competenti in materia

- **Sistemi** di individuazione e analisi delle prove digitali

*Grazie per l'attenzione.*

***Avv. Mario Ianulardo***

***info@codicieleggi.it***

**Università degli Studi di Salerno**

**PENETRATION TESTING AND ETHICAL HACKING**

**14 marzo 2019**