*I crimini informatici:*

*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.*

*Cos’è :*

*Un crimine informatico è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica sia hardware che software. Alcuni crimini in particolare sono finalizzati allo sfruttamento commerciale della rete, a porre a rischio i sistemi informativi di sicurezza nazionale. A livello internazionale, molti governi ed agenzie non governative investono risorse nello spionaggio, nella truffa e in altri crimini transnazionali che coinvolgono interessi economici e politici. La difesa sociale internazionale è impegnata nell'individuare e denunciare tali attori alla Corte Internazionale dell'Aja.*

*Tipi di reati informatici:*

*Il crimine informatico abbraccia un ampio ventaglio di attività suddivise in due categorie:*

*L'utilizzo della tecnologia informatica per compiere l'abuso:*

*-Infezione da virus;*

*-Spam;*

*-Malware (malicious software);*

*L'utilizzo dell'elaboratore nella realizzazione del fatto:*

*-Cyberstalking;*

*-Frode e falsa identità;*

*-Information warfare;*

*-Phishing.*

*Spam:*

*L'inatteso invio di email per fini commerciali è illegale, ma mentre le leggi anti-spam sono relativamente nuove, le comunicazioni inattese esistono da lungo tempo. Spammare significa anche il necropost di un articolo su un forum oppure l'invio ripetuto di messaggi, a volte indesiderati.*

*Frode:*

*La frode informatica è associata alla frode "tradizionale" con la differenza che è realizzata per mezzo di uno strumento informatico. La legge 547 del 1993 aggiunge al Codice Penale l'art. 640-ter per punire chiunque cerchi di ottenere un arricchimento interferendo abusivamente nell'elaborazione dei dati. Non è identificato come frode informatica l'indebito utilizzo di carte di pagamento magnetiche che è invece disciplinato dall'art. 55 del decreto legislativo 231 del 21 novembre 2007. Altri reati previsti sono:*

*-La falsificazione di documenti informatici.*

*-Le aggressioni all’integrità dei dati.*

*-Le aggressioni alla riservatezza dei dati e delle comunicazioni informatiche.*

*Contenuti Sensibili:*

*I contenuti dei siti o altre comunicazioni elettroniche possono essere disattese[vedi discussione], oscene od offensive per molte persone, ma non sempre sono illegali. Oltre venticinque paesi pongono dei severi limiti al riguardo comprese le regole per l'emarginazione di utenti che rispondono ai crimini d'odio, alla blasfemia, alla sovversione politica, alla corruzione di minorenni, all'induzione della prostituzione. La possibilità che queste comunicazioni si diffondano variano da paese a paese e anche all'interno di ogni nazione. Si tratta di un settore dove i Tribunali internazionali possono essere coinvolti per decidere sulle questioni che concernono culture, tradizioni e religioni differenti.*

*Molestie:*

*Mentre alcuni contenuti possono offendere in maniera indiretta, le molestie informatiche possono colpire la sensibilità di chiunque quali commenti sul genere, etnia, religione e orientamento sessuale. Spesso si verificano nelle chat, nei newsgroup, nelle conferenze virtuali, ecc. Circa le aggressioni alle comunicazioni informatiche è ampliato il concetto di corrispondenza contenuto nel quarto comma dell'art. 616 c.p. che ingloba anche la corrispondenza informatica e telematica e punisce l'intercettazione e l'interruzione di comunicazioni informatiche e l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni informatiche , qualora tali condotte non siano esplicitamente autorizzate. La legge 48/08 che recepisce la Convenzione di Budapest sul crimine informatico ha modificato il codice penale e quello di procedura penale riconoscendo implicitamente il ruolo dell'informatica forense nel processo penale.*

*Spaccio di sostanze illecite:*

*I trafficanti di droga stanno ottenendo vantaggi economici tramite messaggi criptati e altre tecnologie virtuali. Gli acquirenti frequentano determinati locali come, ad es., i coffee shop o i milk bar utilizzando siti web finti allo scopo di individuare intere partite di pillole e quantità di anfetamine in chat room. L'aumento dello spaccio via internet potrebbe essere attribuito alla carenza di comunicazioni dirette in modo da stimolare qualsiasi persona ad acquistare la droga. Gli effetti che sono spesso associati allo spaccio di droga, infatti, sono minimizzati e filtrati dai processi che intervengono dall'interazione virtuale.*

*Terrorismo:*

*Agenti governativi e di sicurezza hanno registrato un sensibile incremento dei problemi virtuali sin dal 2001. Ma c'è una buona parte di coloro che ritengono le intrusioni come parte di un disegno terroristico più grande.*

*Un terrorista informatico, quindi, è un individuo o un gruppo di soggetti che, tramite l'attacco informatico, la rete o l'acquisizione segreta di informazioni, ricatta o pone in pericolo un governo o un'azienda al fine di ottenere qualcosa in contropartita per raggiungere i propri fini criminali. Ad es., una innocente propaganda su internet su una fantomatica bomba che esploderà durante un evento o un periodo di tempo, può essere considerato alla stregua di terrorismo informatico. Allo stesso modo, ci sono delle attività illegali dirette verso individui, famiglie, organizzazioni, che tendono a causare panico tra la gente, squilibrare rapporti di forza, raccogliere informazioni rilevanti per la salute della popolazione ed altri simili sconvolgimenti. L'estorsione informatica, in particolare, è una forma di terrorismo informatico nella quale un sito, un'email o un server è soggetto a ripetuti attacchi da parte di hackers al fine di ottenere denaro. Seguendo l'FBI, l'estorsione informatica è in aumento nei confronti di aziende e servizi privati, nella media di venti casi al mese, che si trovano costretti a sborsare milioni di dollari pena l'irrimediabile perdita di tutti i propri dati e sistemi informatici.*