Capitolo I

IL FENOMENO DEL CYBERCRIME COME "PIAGA" MONDIALE.

Sommario: 1.1. La disciplina della criminalità informatica. - 1.2. I soggetti dei reati informatici. - 1.3. Le tipologie dei reati informatici. - 1.4. L'uso di internet tra i minori e la loro protezione. - 1.5. La violazione della privacy come reato informatico. - 1.6. Le possibili conseguenze dei cybercrimes. - 1.7. Il crimine informatico internazionale. - 1.8. "L'acculturazione" dell'utente per la sicurezza e prevenzione informatica.

1.1 La disciplina della criminalità informatica.

Nella realtà virtuale è possibile fare delle cose inconcepibili nel mondo reale, praticamente il mondo virtuale possiede il potenziale per trascendere la realtà.

Fino a qualche anno fa, i reati informatici, sembravano condotte criminose, lontane e incomprensibili, non appartenenti al comune cittadino di qualsiasi Paese, oggi invece rappresentano il nostro presente.

Se prima non conoscevamo il fenomeno del c.d. cybercrime, adesso abbiamo a disposizione tutti gli strumenti utili per comprenderlo a fondo e, semmai fosse necessario, adoperare azioni risolutive o addirittura rivoluzionarie per non restare nello "*status quo*".

(Senza rendercene conto), Viviamo tra la manipolazione delle multinazionali elettroniche e la necessaria esigenza dell'uso della rete informatica nonché "dell'andare al passo coi tempi" riguardo a ciò.

Come se si fosse perduto, in un certo senso, il controllo del "mondo virtuale", della navigazione in generale, e di tutto quello che è connesso all'informatica, dimenticando che la rete e i mezzi informatici nascono per mano dell'uomo, e da quest'ultimo, perciò, controllabili.

Nonostante tutto, la "rete" sta sovrastando la vita sociale e questo accade perché diamo sempre più importanza al mondo virtuale, fino a portarlo in quello reale, quasi a sostituire la vita reale con quella virtuale o comunque a confondere le due realtà diverse, ignorando che quella che ci resta, una volta disconnessi dalla rete, è proprio la vita reale.

Non è un caso se si sono evoluti i crimini informatici, visto l'uso che ne facciamo di internet.
Se ci chiediamo: "esiste un diritto penale dell'informatica?", dovremmo risponderci: sì, sarebbe bello se ci fosse, ma non esiste purtroppo.

Infatti, la disciplina dei reati informatici, quindi della criminalità informatica, è inserita in vari testi di legge non collegati tra loro, e altre norme si trovano "sparse" per il Codice penale italiano; dunque, non c'è ad oggi un corpus normativo unitario che regoli l'intero istituto della criminalità informatica.

Attualmente la legge che disciplina i reati informatici è la legge n 48/2008 ma dobbiamo premettere che prima di arrivare a questa, nota come la ratifica della Convenzione di Budapest[1], o più precisamente: Legge 18 marzo 2008, n. 48

[1] estensione delle norme penali in materia di reati informatici, *L. 48/2008* (parlamento.it).

"Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno", che si è avuta con ritardo rispetto al previsto, è entrata in vigore nel 2008 ed ha introdotto numerose modifiche alle disposizioni penali in tema di reati informatici ed in merito alla disciplina processuale sulle indagini relative a tali crimini.

La suddetta legge è così composta:

Capo I – RATIFICA ED ESECUZIONE

Art. 1. *autorizzazione alla ratifica*;

Art. 2. *ordine di esecuzione*;

Capo II – MODIFICHE AL CODICE PENALE E AL DECRETO LEGISLATIVO 8 GIUGNO 2001, N 231

Art. 3. *modifiche al titolo VII del libro secondo del Codice penale;* (ad esempio: falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri);

Art. 4. *modifica al titolo XII del libro secondo del Codice penale;* (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico);

Art. 5. *modifica al titolo XIII del libro secondo del Codice penale* (ad esempio: danneggiamento di informazioni, dati e programmi informatici)

Art. 6. *modifiche all'articolo 420 del c.p.;* (il secondo e terzo comma sono stati abrogati);

Art. 7. *introduzione dell'art. 24 bis del decreto legislativo 8 giugno 2001, n. 231;* (delitti informatici e trattamento illecito di dati)

Capo III – MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

Art. 8. *modifiche al titolo III del libro terzo del codice di procedura penale;* (ad esempio: sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni);

Art. 9. *modifiche al titolo IV del libro quinto del codice di procedura penale;* (ad esempio, al comma 3 dell'art. 353 c.p. si sostituisce quanto segue: "lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica");

Art. 10. *modifiche all'art. 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196;*

Art. 11. *Competenza*;

Art. 12. *Fondo per il contrasto della pedopornografia su* internet *e per la protezione delle infrastrutture informatiche di interesse nazionale;*

Capo IV – DISPOSIZIONI FINALI

Art. 13. *Norma di adeguamento;*

Art. 14. *Entrata in vigore.*[2]

Prima dell'attuale l. n. 48/2008, si è pensato di provvedere alla mancanza di sanzioni penali, per i comportamenti di cybercrime, con la legge n. 547 del 1993[3]: Considerando che prima di tale periodo esisteva la criminalità informatica come reato, ma non esisteva una conseguenza sanzionatoria per queste condotte criminose, in quanto difficile da attuarsi.

La legge n. 12 del 15/02/2012[4], invece ha disciplinato le nuove misure per contrastare i fenomeni di criminalità informatica, soprattutto con l'art. 1 si è introdotto una importante modifica dell'art 240 c.p., introducendo la confisca dei beni e degli strumenti informatici o telematici che risultino essere stati in tutto o in parte utilizzati per la commissione dei reati introdotti con le l. n. 547/1993 e l. n. 48/2008.

1.2 I soggetti dei reati informatici.

Generalmente, chiunque svolge attività attinente al funzionamento del sistema informatico e alle misure di sicurezza poste a protezione dello stesso, nonché alla sua cura, è l'amministratore.

[2] pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 - Supplemento ordinario n.79.
[3] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1993-12-23;547.
[4] L. 15 febbraio 2012, n. 12 - Normattiva, L. 12 del 2012.pdf (penalecontemporaneo.it).

Possono essere configurabili, nell'ambito del cyberspazio e cybercrime, diversi soggetti preposti in base alle operazioni finali destinate: - l'operatore di sistema; - il programmatore, - il sistemista, - l'analista.

Utilizzare un insieme di tecniche ed operazioni volte a conoscere, accedere, e modificare un sistema informatico (hardware e software), per incrementare alcune prestazioni, oppure rimuovere limitazioni al funzionamento di alcuni componenti elettronici o di applicazioni o l'aggiungere funzioni ad un programma, è lecito.

Ma quando si utilizzano certe conoscenze tecniche per aggirare l'acquisto delle licenze, per esempio, o per accedere ai sistemi altrui, con lo scopo di impadronirsi dei dati riservati presenti o di danneggiare il funzionamento, costituiscono espressione di reati informatici.

L'aggressione ai sistemi informatici e telematici è solitamente realizzata da soggetti con elevate conoscenze e capacità tecnico-informatiche, che vengono definiti hacker e cracker. Recentemente autori come Braid e Ranauro, hanno proposto una classificazione differente sulla base della diversa struttura del comportamento e delle diverse motivazioni. Secondo questi ultimi autori, mentre gli hacker attribuiscono ad una informazione, qualunque essa sia, lo stesso valore ad essa attribuito del proprietario delle informazioni stesse, i cracker sono veri e propri "info-maniacs", persone che ricercano le informazioni in maniera praticamente ossessiva. Nella loro sub-cultura l'informazione è "moneta di scambio" per accumulare un sempre maggior numero di informazione e di dati,

come numeri di telefono, passwords, numeri di conto, metodi per eludere le misure di sicurezza e penetrare nei sistemi ecc...

L' hacker, dunque, pratica l'attività di hacking[5] e ha come obiettivo quello di acquisire un'accurata padronanza del sistema su cui interviene per adattarlo alle sue esigenze.

Il cracker invece, pratica l'attività di cracking[6] attraverso una tecnica chiamata "reverse engineering", ovvero un'operazione che permette di comprendere il funzionamento del software che si intende violare analizzando le risposte che quest'ultimo fornisce a determinati input.

All'art. 21 (Sanzioni)[7], d.lgs. 9/04/2003 n. 70 stabilisce che:

1. Salvo che il fatto costituisca reato, le violazioni di cui agli articoli 7, 8, 9, 10 e 12 sono punite con il pagamento di una sanzione amministrativa pecuniaria da 103 euro a 10.000 euro.

2. Nei casi di particolare gravità o di recidiva i limiti minimo e massimo della sanzione indicata al comma 1 sono raddoppiati.

3. Le sanzioni sono applicate ai sensi della legge 24 novembre1981, n. 689. Fermo restando quanto previsto in ordine ai poteri di accertamento degli ufficiali e degli agenti di polizia giudiziaria dall'articolo 13 della citata legge 24 novembre

[5] F. Peluso (a cura di), *la responsabilità nei nuovi reati informatici, mezzi di ricerca e acquisizione della prova*, Maggioli, Santarcangelo di Romagna, 2020, p.129.
[6] F. Peluso (a cura di), *la responsabilità nei nuovi reati informatici*, Maggioli, Santarcangelo di Romagna, 2020, pp. 129-130.
[7] d.lgs. 9 aprile 2003, n. 70 - Normattiva.

1981, n. 689, all'accertamento delle violazioni provvedono, d'ufficio o su denunzia, gli organi di polizia amministrativa. Il rapporto di accertamento delle violazioni di cui al comma 1 è presentato al Ministero delle attività produttive, fatta salva l'ipotesi di cui all'articolo 24 della legge 24 novembre 1981, n. 689.

1.3 Le tipologie dei reati informatici.

L'avvento delle tecnologie informatiche e telematiche ha determinato la nascita di fenomeni come l'e-commerce, l'e-government, l'home banking e tante altre attività. Oggi la maggior parte delle attività sociali, lavorative e di svago avvengono con l'ausilio di un elaboratore elettronico. Quanto detto vale sia per le attività di natura lecite, sia per quelle illecite. I reati informatici possono quindi, essere definiti come il risvolto negativo dello sviluppo tecnologico dell'informatica e della telematica[8].

La Convenzione di Budapest (23/11/2001), ha suggerito, attraverso gli artt. 2-10, l'introduzione di misure legislative atte a sanzionare alcune condotte tipiche di aggressione ai sistemi informatici, come fattispecie di: *accesso abusivo, intercettazione illegale, attentato all'integrità dei dati e dei sistemi, abuso di apparecchiature, falsificazione informatica, pornografia infantile e violazione della proprietà intellettuale.*[9]

[8] F. Corona, *Manuale di diritto di internet, le principali ed innovative tematiche dell'informatica giuridica: ambito civile, penale, amministrativo, e le tecnologie emergenti,* EPC, 2021.
[9] Cfr. L 48/2008 (parlamento.it).

L'art. 640 ter c.p. punisce l'illecito arricchimento conseguito con l'impiego fraudolento di un sistema informatico. Il raggiro al sistema informatico può configurarsi in una qualsiasi delle fasi del processo di elaborazione dei dati posto in essere dall'elaboratore: durante la fase iniziale di raccolta e di inserimento dei dati da elaborare, durante la fase di elaborazione in senso stretto, oppure durante la fase di emissione dei dati elaborati. L'art. 491 bis del c.p., estende ai documenti informatici pubblici o privati, aventi efficacia probatoria (come disciplinato dalla l. n. 48/2008), la medesima disciplina prevista per le falsità commesse con riguardo ai tradizionali documenti cartacei, punite dagli artt. 476 e 493 c.p.; il codice penale regolamenta la categoria dei reati di integrità dei dati e dei sistemi informatici, all'art. 635-bis, disciplinato nel libro II, "d*elitti in particolare*", titolo XIII, "*dei delitti contro il patrimonio*", capo I "*dei delitti contro il patrimonio mediante violenza alle persone*". Altresì si rinviene tutela nell'art. 615-quinquies, disciplinato nel c.p. nel libro II "*delitti in particolare*", titolo XII "*delitti contro la persona*", capo III "*dei delitti contro la libertà individuale*", sez. III "*dei delitti contro la libertà morale*". Infine il codice penale, relativamente alla riservatezza dei dati e delle comunicazioni informatiche, mira alla repressione delle forme di intrusione nella sfera privata altrui; il primo intervento previsto a partire dalla l. 547/1993 in materia di riservatezza dei dati e delle comunicazioni informatiche, sono quelli relativi agli artt. Che vanno dal 615-ter c.p. al 615-sexies c.p., tutti

inseriti nel titolo XII "*dei delitti contro la persona*", capo II "*dei delitti contro la libertà individuale*", sez. IV "*dei delitti contro l'inviolabilità del domicilio*".[10]

1.4 L'uso di internet tra i minori e la loro protezione.

I minori nella rete sono sempre più connessi tramite smartphone e sempre più attivi sui social; a dimostrarlo è il Report "Digital 2020", pubblicato da *we are social e hootsuite*, che fornisce un resoconto sullo scenario digitale, analizzando i dati raccolti in 239 Paesi, offrendo una visione globale sulla diffusione della rete e sull'uso dei moderni strumenti di comunicazione telematica; invece a livello nazionale sono quasi 50 milioni le persone online ogni giorno e 35 milioni quelle attive sui canali social, con un trend in crescita per quanto riguarda internet, piattaforme social e nuove tecnologie.[11]

I problemi sorgono quando i comportamenti diventano illeciti, considerando anche il fatto che con l'uso della rete non ci sono più confini e quindi non esistono limiti territoriali e temporali.

La tutela dei minori è avvenuta con un processo graduale di livelli di protezione, dapprima si partiva con la concezione che il bambino fosse solamente un soggetto titolare di diritti, fino ad arrivare, poi, alla visione di un soggetto bisognoso di particolare tutela in virtù della sua età e dunque della sua immaturità fisica ed

[10] Cfr. F. Corona, *Manuale di diritto di internet, le principali ed innovative tecniche,* EPC, 2021.
[11] Report Digital 2020: lo scenario nel mondo e in Italia (digitaldictionary.it).

intellettuale. Uno dei primi strumenti di protezione del minore, in ordine cronologico, fu la *Dichiarazione dei diritti del fanciullo:* un documento redatto a Ginevra il 23 febbraio 1923 dalla Società delle Nazioni in seguito alle conseguenze prodotte dalla Prima guerra mondiale sui bambini. Venne adottata dall'Assemblea Generale della Società delle Nazioni nel 1924. L' Italia ratificò questa legge nel 20 novembre 1989.[12]

Un secondo strumento di protezione del minore è la *Convenzione sull'età minima,* a tutela dei diritti dell'infanzia, adottata a Ginevra, dalla conferenza internazionale del lavoro nel 1919.[13] La convenzione riconosce un ruolo sempre più rilevante ai nuovi mezzi di comunicazione, poiché questi assumono una delicata funzione educativa che va ad affiancare, e talvolta a sostituire, quelle tradizionali della famiglia e della scuola. Per cui sussiste l'esigenza di bilanciare diversi diritti fondamentali: - la tutela dei minorenni nell'ambito dell'uso sicuro delle tecnologie dell'informazione (art. 17 CRC); - il diritto all'informazione e la libertà di espressione (art. 13 CRC); - l'obbligo degli stati di garantire ai genitori di poter svolgere congiuntamente il loro diritto/dovere di proteggere ed educare i figli (art. 8 CRC); - il diritto di essere protetti da abusi sessuali (art. 34 CRC). [14] [...]

[12] Convenzione_1959.pdf (savethechildren.it).
[13] Convenzione sull'età minima, 1973 (ilo.org).
[14] Unicef, *Protecting the World's Children: Impact of the Convention on the Rights of the Child in Diverse Legal System*, Cambridge University Press, 2008.
Gli articoli della Convenzione | UNICEF Italia; convenzione diritti minori - semplificata.pdf (ismu.org).