UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di diritto pubblico, internazionale e comunitario

CORSO DI LAUREA IN

DIRITTO E TECNOLOGIA

TESI DI LAUREA

PREVENZIONE E REPRESSIONE DEI REATI INFORMATICI

RELATORE: Prof. Massimo Bolognari

STUDENTE: Sofia Cecchetto

MATRICOLA: 2001750

ANNO ACCADEMICO 2022 / 2023

Alla stella più luminosa,
mia zia Ornella

INDICE

CAPITOLO 1 9
I REATI INFORMATICI 9
1. La digitalizzazione 9
2. I reati informatici 10
3. I reati informatici comuni 11
4. I reati comuni a mezzo informatico 13
5. I reati informatici nel d.lgs. 231/2001 14
CAPITOLO 2 17
PREVENZIONE DEI REATI INFORMATICI 17
1. Introduzione alla prevenzione 17
2. Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche .. 18
3. Accordo sulla prevenzione 19
4. Come riconoscere e come proteggersi da un crimine informatico? 20
5. Soggetti attivi e responsabilità 22
6. Prevenzione nel d.lgs. 231/2001 23
CAPITOLO 3 25
REPRESSIONE DEI REATI INFORMATICI 25
1. La denuncia di un crimine informatico 25
2. La Polizia Postale e la sua organizzazione 26
3. Come agisce la Polizia Postale? 27
4. L'individuazione del giudice competente 27
5. Come vengono puniti i reati informatici? 28
CAPITOLO 4 31
I REATI INFORMATICI A LIVELLO EUROPEO E NEL MONDO 31
1. L'a-territorialità 31
2. Un quadro europeo 32
3. Un quadro extraeuropeo 33
CONCLUSIONE 35
BIBLIOGRAFIA 37
SITOGRAFIA 38

INTRODUZIONE

La rivoluzione tecnologica degli ultimi sessant'anni ha avuto un impatto travolgente in tutti gli ambiti della società in cui viviamo. I mezzi informatici di cui oggi disponiamo consentono di svolgere qualsiasi attività in modo automatizzato, grazie ad un semplice '*click'* su dispositivi che, nella maggior parte dei casi, sono grandi come la nostra mano.

L'obiettivo del presente lavoro è quello di analizzare la digitalizzazione sulla prevenzione e sulla repressione dei reati informatici.

Nel primo capitolo, si è analizzato il fenomeno della digitalizzazione, che consiste nella trasformazione dei dati e dei processi analogici in digitale e gli effetti che essa comporta. Ci si è poi soffermati sui i crimini informatici, che consistono nel compimento di un reato attraverso gli strumenti digitali, distinguendo i reati informatici , come, ad esempio, l'accesso abusivo ad un sistema informatico, dai reati comuni commessi a mezzo informatico, come, ad esempio, il cyberbullismo, focalizzandosi infine sulla peculiare ipotesi della responsabilità dell'ente rispetto alla commissione di reati informatici.

Nel secondo capitolo, invece, ci si è concentrati sull'attività di prevenzione dei crimini informatici, analizzando, in particolare, la posizione ricoperta dall'ente e dal provider.

Nel terzo capitolo si sono esaminati, invece, i vari organismi e le varie istituzioni che intervengono per la repressione dei reati informatici.

Infine, alla luce della natura tendenzialmente transnazionale dei reati informaci, si sono esaminati i problemi relativi alla cooperazione in materia penale sia in ambito europeo sia in una dimensione internazionale.

CAPITOLO 1

I REATI INFORMATICI

1. La digitalizzazione

La nostra vita sta cambiando e questo processo evolutivo diventa sempre più veloce. Siamo all'interno di una rivoluzione digitale che sta modificando il nostro modo di essere nel mondo, la nostra percezione della realtà, le diverse sfumature dell'identità, le relazioni sociali, il piccolo mondo in cui viviamo in relazione alla globalità dell'universo. Risulta quindi necessario confrontarsi con questa realtà in continua evoluzione.

La digitalizzazione consiste nella trasformazione di dati e processi analogici in forma digitale. La realtà è diventata una realtà fatta di BIT[1]; al riguardo il fisico Melvin M. Vopson ha rilevato che "attualmente, produciamo circa 10^{21} bit digitali di informazioni ogni anno sulla Terra. Ipotizzando un tasso di crescita annuo del 20%, stimiamo che tra circa 350 anni, il numero di bit prodotti supererà il numero di tutti gli atomi sulla Terra, all'incirca 10^{50}". [2]

Si è iniziato a parlare di digitalizzazione negli anni Cinquanta, grazie all'avvento dei primi computer; alla fine degli anni Novanta, la rivoluzione digitale è diventata una realtà globale, dal momento che in tutti i paesi iniziava ad essere presente una connessione ad Internet. Tutto il mondo quindi risulta connesso e le informazioni viaggiano in un modo sempre più veloce ed istantaneo.

---

[1] BIT: cifra binaria; cifra del sistema di numerazione binario. Nella teoria dell'informazione e in informatica, esso rappresenta l'unità di misura del contenuto di informazione di un messaggio.

[2] www.servicematica.com → La catastrofe dell'informazione: nel futuro il nostro corpo sarà fatto di bit?

2. I reati informatici

Lo sviluppo delle tecnologie informatiche ha determinato nuovi e inediti scenari. La maggior parte delle attività umane che venivano svolte manualmente o mediante apparecchiature meccaniche viene oggi svolta dalle nuove tecnologie digitali. Questo fenomeno va senz'altro salutato positivamente. Si pensi solo alla maggior efficienza, velocità e semplificazione dei vari processi[3]. Tuttavia, occorre tenere presenti anche i rischi che sono correlati alla digitalizzazione. Poiché le attività e gli interessi si spostano su Internet, anche le attività illecite seguono la stessa impronta.

Questi mezzi moderni, protagonisti della c.d. rivoluzione digitale, garantiscono la possibilità di commettere crimini molto sofisticati, come i reati informatici. I reati informatici non sono altro che crimini compiuti mediante l'utilizzo di supporti informatici, digitali o telematici. Pertanto, viene ritenuta reato informatico, la condotta prevista e punita dal Codice Penale (e da altre varie legislazioni speciali) che vede il supporto informatico l'elemento principale per la qualificazione del fatto di reato.[4]

La maggior parte delle relazioni che intratteniamo durante la nostra quotidianità avvengono per lo più in modalità telematica. Ci si riferisce, in particolare, ai telefoni cellulare, ai computer, tablet e tutti gli altri dispositivi che ci permettono di essere a stretto contatto con i nostri dati, ma anche con quelli degli altri. La *privacy* di ognuno di noi è messa costantemente a rischio. Infatti, si constata che nei *cybercrime* la difficoltà di un intervento da parte del legislatore veloce ed efficace risulta proporzionale alla velocità con la quale si sviluppano gli strumenti di difesa.[5]

È necessario quindi, in funzione di tali criticità, che lo sviluppo tecnologico abbia una normativa adatta che risulti al passo con le nuove e costanti rivoluzioni che si presentano nel

---

[3] Si pensi allo sviluppo di attività, quali e-commerce, e-government, home-banking.

[4] https://www.riskmanagement360.it/cybersecurity/sicurezza-informatica-e-d-lgs-231-come-proteggersi-dalla-responsabilita-penale/

[5] *L. LUPARIA, Sistema penale e criminalità informatica, 2009, p.83*

nostro mondo, in modo tale da poter essere sempre al passo, tutelando anche i futuri ed imprevedibili reati informatici.

3. I reati informatici comuni

Abbiamo visto nel paragrafo precedente che il reato informatico è un tipo di condotta illecita che comporta l'uso improprio di componenti hardware e software del computer. Il crimine informatico è una tipologia di crimine condotto dai criminali informatici, chiamati, in gergo, pirati informatici o hacker[6].[7]

I reati informatici comuni sono suddivisi in cinque categorie:

- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche,
- Detenzione e diffusione abusiva di codici di accesso a sistemi;
- Diffusione di hardware e software diretti a danneggiare sistemi;
- Accesso abusivo a un sistema informatico;
- Frode informatica.

Vediamo alcune caratteristiche correlate a ciascun crimine.

Intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche senza autorizzazione (Art. 617-quater c.p.): tale norma punisce "chiunque in modo fraudolento intercetta, inibisce o interrompe comunicazioni connesse a un sistema informatico o telematico o tra più sistemi". Un chiaro esempio è l'intercettazione dei dati di navigazione attraverso l'utilizzo di una rete Wi-Fi libera.[8]

Detenzione e diffusione abusiva di codici di accesso al sistema (Art. 615-quater c.p.): chiunque abusivamente ottenga, riproduca, diffonda, comunichi o recapita codici o altri

[6] Hacker: persona non violenta e solitaria, dotata di grande capacità di pianificazione del comportamento che intende sfruttare le proprie conoscenze informatiche per raggiungere i suoi obiettivi.
[7] https://www.onoratoinformatica.it/sicurezza-cibernetica
[8] ivi

mezzi idonei ad accedere ad un sistema informatico protetto da misure di sicurezza, commette un crimine informatico.[9]

Diffusione di hardware e software diretti a danneggiare il sistema (Art. 615- quinquies c.p.): chiunque ottenga, produca, riproduca o metta a disposizione apparecchiature, dispositivi o programmi informatici con l'intento di danneggiare illecitamente un sistema informatico e mette a disposizione programmi per favorire l'interruzione o l'alterazione di un sistema informatico viene punito dalla legge. Degli esempi sono gli attacchi malware di diversa natura, tra cui spyware[10] e trojan[11].[12]

Accesso abusivo ad un sistema informatico (Art. 615-ter c.p.): rientra in questa categoria l'accesso non autorizzato ai social network, ai conti e-banking utilizzando le credenziali del titolare a sua insaputa. Importante notare che il fatto di reato è già stato compiuto eseguendo l'accesso illegalmente, senza tenere conto che, una volta eseguito l'accesso, l'utente hacker potrebbe compiere ulteriori reati informatici.[13]

Frode informatica (Art. 640-ter c.p.): viene definita frode informatica la condotta di chi "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."[14] Il reato più comune di questa categoria è il *phishing*, ossia una sorta di sollecitazione in cui il cybercriminale inganna l'utente al fine di ottenere informazioni importanti, come password e documenti d'identità. Vi è poi la proliferazione dei *dialer*, applicazioni che, una volta scaricate su un pc o un telefono, interrompono la

[9] https://www.onoratoinformatica.it/sicurezza-cibernetica
[10] Spyware: Software scaricato, spesso in maniera inconsapevole, durante la navigazione in Internet o l'installazione di un software gratuito, programmato per registrare e trasmettere a terzi dati personali e informazioni sull'attività online di un utente, generalmente a scopo pubblicitario.
[11] Trojan: Software che può essere installato all'insaputa del destinatario in un dispositivo impiegato dal dispositivo.
[12] https://www.onoratoinformatica.it/sicurezza-cibernetica
[13] ivi
[14] Def. Brocardi

connessione con l'operatore designato e si collega ad un altro operatore ad insaputa dell'utente-vittima.[15]

Sono presenti nel nostro ordinamento ulteriori reati informatici contemplati dalla Legge 574/1993[16]. La gamma dei possibili attacchi informatici è molto vasta e l'UE, nella "Raccomandazione" del 13/09/1989 (integrata poi nel 1994), ne elenca ben 14 tipologie, che in dottrina vengono raggruppati in due categorie:

- Utilizzo della tecnologia informatica per compiere l'abuso: spam, malware;
- Utilizzo della tecnologia informatica nella realizzazione del fatto criminoso: cyberstalking, frode informatica, falsa identità, information warfare e phishing.

4. I reati comuni a mezzo informatico

Vediamo ora una categoria di reati che possono essere commesse anche offline, ma nel momento in cui vengono commessi tramite il web assumono una connotazione informatica.

Il *Cyberbullismo*: il bullismo è un tema di grande attualità. Di rado si sente parlare di quello che viene commesso nelle scuole, ma sempre più si parla di quello commesso attraverso *chat* e *social media*. Il cyberbullismo consiste nell'insieme di azioni aggressive e intenzionali, di una singola persona o di un gruppo, realizzate mediante strumenti elettronici, come sms, mms, *email, chat rooms, siti web*, telefonate, il cui obiettivo è quello di provocare danni ad un coetaneo incapace di difendersi.[17]

La *pedopornografia*: viene utilizzata, in questo caso, la rete web per il traffico di immagini o video a contenuto pedopornografico. Tale reato non è aggravato dall'utilizzo della

[15] https://www.onoratoinformatica.it/sicurezza-cibernetica
[16] Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica
[17] https://www.miur.gov.it/bullismo-e-cyberbullismo

tecnologia, ma, di fatto, la tecnologia ne ha facilitato la diffusione e ha portato ad un aumento esponenziale di crimini di tale tipologia.

La *diffamazione*: la diffamazione si ha quando, comunicando con più persone, viene offesa la reputazione di un'altra persona.

La *violazione del copyright*: tale reato avviene quando vengono danneggiati i diritti dell'autore dell'opera attraverso il plagio, la riproduzione dell'opera a fini commerciali, la modifica senza autorizzazione.

5. I reati informatici nel d.lgs. 231/2001

Una delle novità più rilevanti degli ultimi anni riguarda la previsione di una forma di responsabilità anche delle persone giuridiche. Il d.lgs. 231/2001 ha introdotto una nuova forma di responsabilità "da reato", la quale deriva dalla commissione (o tentata commissione) di una serie di reati commessi da amministratori, dirigenti, dipendenti o terzi mandatari, qualora siano stati realizzati nell'interesse o a vantaggio dell'impresa e siano stati resi possibili da carenze della struttura organizzativa dell'impresa stessa. La scelta di far ricadere la responsabilità sull'impresa stessa dipende dal fatto che alcuni illeciti sono ascrivibili non tanto al singolo autore, ma all'ente nel suo complesso, dal momento che all'interno di una struttura organizzativa vi sono molteplici apparati ed il processo decisionale è scandito in base ad una varietà di fasi governate da diversi gruppi.[18]

Inizialmente, al momento della sua emanazione, il d.lgs. 231/2001 prevedeva solamente il reato di frode informatica. Successivamente, con l'introduzione della legge 48 del 2008[19], l'art. 24 *bis*, rubricato "Delitti informatici e trattamento illecito di dati", inserisce all'interno anche i reati informatici, creando il collegamento tra il decreto 231 e il tema della *cybersecurity*.

[18] https://assistenza-legale-imprese.it/d-lgs-n-231-2001-responsabilita-enti/
[19] "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informativa, fatta a Budapest il 23 novembre 2001 e norme di adeguamento dell'ordinamento interno". Pubblicata nella Gazzetta Ufficiale n. 80 del 4 aprile 2008 – supplemento ordinario n.79

I reati informatici che coinvolgono gli enti sono una realtà che colpisce tutte le organizzazioni, indipendentemente dalle dimensioni. Per avere una migliore comprensione, è utile distinguere tali reati informatici in tre categorie:

- Reati informatici compiuti dai propri dipendenti a danno dell'organizzazione, come per esempio, furto di dati aziendali, che si verifica quando un dipendente esegue copie illegali di dati archiviati nei sistemi aziendali per un uso illegale; oppure quando un dipendente preleva dei dati aziendali e li trasferisce ad un concorrente, o addirittura, quando un ex dipendente della società conserva dati a lui forniti per l'esecuzione del suo lavoro e li utilizza per creare un'impresa in concorrenza con il precedente datore di lavoro;[20]
- Reati informatici compiuti da soggetti esterni a danno dell'organizzazione; le minacce più comuni contro le aziende sono gli attacchi ransomware[21] e gli attacchi phishing;
- Reati informatici compiuti a vantaggio dell'organizzazione dai propri dipendenti. In tale caso, la responsabilità è limitata ai reati specificamente definiti dalla legge. In particolare, l'articolo 24-bis del D.lgs. 231/2001 prevede l'accesso non autorizzato ad un sistema informatico o telematico; il danneggiamento di informazioni, dati e programmi impiegati dallo Stato o da altri enti pubblici; la diffusione di apparecchiature, dispositivi o programmi con l'intento di danneggiare un sistema informatico.[22]

[20] https://www.onoratoinformatica.it/sicurezza-cibernetica
[21] programma informatico dannoso che può "infettare" un dispositivo digitale, bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un riscatto (in inglese, "ransom") da pagare per "liberarli".
[22] https://www.onoratoinformatica.it/sicurezza-cibernetica

CAPITOLO 2

PREVENZIONE DEI REATI INFORMATICI

1. Introduzione alla prevenzione

Prevenire un crimine informatico è un'attività molto complessa, in quanto non bisogna considerare soltanto la stretta connessione che vi è fra i vari reati possibili, ma è necessario comprendere la capacità e la competenza informatica posseduta da coloro che intendono delinquere.

Inoltre, occorre evidenziare come nessun sistema sia completamente sicuro: vi è un minimo livello di sicurezza, determinato da un bilanciamento di vari elementi, come l'investimento economico che si è disposti a sostenere, il livello di rischio che si è disposti a tollerare e quanto si intende difendere.

Sicuramente non possiamo prevedere un controllo accurato per ogni singola attività, ma possiamo mettere in atto comportamenti più generali che fanno riferimento ad una pluralità di atti, in modo tale da garantire un controllo più efficace.

Al giorno d'oggi per comprendere meglio il concetto e trovare una soluzione ad hoc per fronteggiare le nuove forme di criminalità e per eseguire un'armonizzazione delle fattispecie, diventa necessario prendere in considerazione i concetti di "dato informatico" e di "sistema", in relazione ai quali si tratteggiano le condotte criminose.[23]

È importante conoscere le varie definizioni per provare a comprende al meglio la dimensione del fenomeno del cybercrime: il sistema, infatti, viene definito con "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*"[24]; per dato informatico, invece, si intende "*any representation of facts, information or concepts in a form suitable for processing in a computer system,*

[23] *L. LUPARIA, Sistema penale e criminalità informatica, 2009, p.92*

[24] Def: "qualsiasi dispositivo o gruppo di dispositivi interconnessi o connessi, uno o più dei quali, ai sensi di un programma, esegue il trattamento automatico dei dati".

including a program suitable to cause a computer system to perform a function"[25]. Tali definizioni risultano necessarie da un lato per non ostacolare i mezzi elettronici dotati di software o firmware che permettono allo stesso di lavorare elaborando informazioni o comandi tra gli strumenti attraverso i quali è possibile portare a compimento reati informatici, dall'altro per predisporre tutele penalistiche create appositamente sui dati, quindi su singoli *files*.[26]

2. Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) è "il soggetto incaricato della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale".[27]

Il C.N.A.I.P.I.C., avvalendosi di tecnologie di elevato livello e di personale altamente qualificato specializzato nel contrasto del cybercrime, svolge la sua attività attraverso alcune funzioni, quali:

- Sala operativa, punto di contatto univoco, disponibile 24 ore su 24 e 7 giorni su 7, dedicato allo scambio di informazioni;
- *Intelligence*, ossia la raccolta dei dati e delle informazioni utili ai fini di prevenzione, attraverso il costante monitoraggio su internet, sia a livello nazionale che internazionale ed in virtù dei consolidati rapporti di collaborazione operativa e condivisione informativa con gli altri organismi di polizia, gli enti e le aziende impegnati nei settori dell'*ICT security*;

[25] Def: qualsiasi rappresentazione di fatti, informazioni o concetti in una forma idonea all'elaborazione in un sistema informatico, compreso un programma atto a indurre un sistema informatico a svolgere una funzione.
[26] L. LUPARIA, Cybercrime e responsabilità degli enti. A cura di Luca Luparia, Varese, Giuffrè editore, 2009, p. 92
[27] https://www.commissariatodips.it/profilo/cnaipic/index.html

- Analisi, che consiste nella comparazione dei dati e delle informazioni raccolte, predisposizione di rapporti previsionali sull'evoluzione della minaccia e delle vulnerabilità informatiche, delle tecniche e delle iniziative criminali;
- Investigazione, ovvero intervento operativa al verificarsi di un evento informatico criminale. Collabora anche con organismi di polizia stranieri e internazionali, come Interpol, Europol.

Il valore aggiunto che tale Centro rappresenta nell'ambito della protezione delle Infrastrutture Critiche (I.C.), deriva dalla realizzazione della Sala Operativa disponibile 24/7, in veste di punto di contatto univoco impegnato nella protezione delle I.C. e dai collegamenti telematici esclusivi tra il C.N.A.I.P.I.C. e le Infrastrutture Critiche, per la costante condivisione ed il costante trasferimento dei dati e delle informazioni utili all'esercizio delle funzioni di valutazione, prevenzione e repressione delle minacce e dei crimini informatici.[28] [29]

3. Accordo sulla prevenzione

Il 6 luglio 2023, a Roma, è stato siglato dalla Polizia di Stato e da Anci (Associazione Nazionale Comuni Italiani) l'accordo sulla prevenzione e il contrasto dei crimini informatici sui sistemi informativi dei Comuni Italiani.

Tale Protocollo prevede che le attività connesse alla tutela dei sistemi e dei servizi informatici critici vengano assicurate dalla Polizia Postale e delle Comunicazioni e dal C.N.A.I.P.I.C., che, come abbiamo visto prima, rappresenta con la sua sala operativa aperta 24/7 il punto di contatto nazionale per la gestione degli eventi critici alle infrastrutture di rilievo nazionale.[30]

L'iniziativa si inserisce in un contesto di generale rinnovamento e crescita delle strutture territoriali della Polizia Postale e conferma il costante impegno nella creazione di una rete di

[28] https://www.commissariatodips.it/profilo/cnaipic/index.html
[29] https://www.interno.gov.it/it/temi/sicurezza/crimine-informatico/centro-nazionale-anticrimine-informatico-protezione-infrastrutture-critiche-cnaipic
[30] https://www.commissariatodips.it/notizie/articolo/polizia-di-stato-e-anci-siglano-laccordo-sulla-prevenzione-e-il-contrasto-dei-crimini-informatici-s/index.html

collaborazione sempre più solida e strutturata. Tutto ciò è avvenuto nell'ottica di garantire livelli di azione sempre più rapidi, elevati e qualificati, contribuendo al contenimento dei costi operativi derivanti da interruzioni dei servizi erogati, tutelando la privacy dei cittadini attraverso l'innalzamento degli standard di protezione delle banche dati sensibili a cui accedono le amministrazioni comunali.[31]

4. Come riconoscere e come proteggersi da un crimine informatico?

Come abbiamo visto nel capitolo precedente, moltissime attività si sono spostate dai luoghi fisici alla rete. Pensiamo agli e-commerce, all'home-banking, al trading online e a tutti i passaggi di documenti che una volta avvenivano mediante posta cartacea e, oggi, tramite il web. Inoltre, lo sviluppo massivo del lavoro da remoto, il c.d. smart working, ha comportato il trasferimento di un vasto numero di documenti via web. Tutto ciò ha comportato l'aumento esponenziale dei reati informatici; se da un lato la digitalizzazione ha fatto in modo che molte attività subissero una significativa semplificazione, al contrario abbiamo lo sviluppo di illeciti che si consumano attraverso il web e mediante il computer come sistema di conservazione dei dati.

Per riconoscere un crimine informatico, le modalità variano in base alla tipologia del reato commesso. Ad esempio, ci si può rendere conto che è stato introdotto un malware all'interno del computer dai rallentamenti del sistema e dai messaggi di errore visualizzati. Oppure, per riconoscere la presenza di keylogger (programmi che riescono a leggere e registrare ciò che digitiamo sulla tastiera), è possibile capirlo dalla presenza di segni distintivi, come messaggi duplicati. Ancora, per riconoscere gli attacchi phishing, bisogna essere nella condizione di riconoscere le mail fraudolente da quelle reali ed innocue.

Alcune tecniche a cui affidarsi per evitare di incorrere in queste "trappole" possono essere: controllare l'autenticità delle mail, quindi verificare innanzitutto il mittente della email prima

[31] https://www.commissariatodips.it/notizie/articolo/polizia-di-stato-e-anci-siglano-laccordo-sulla-prevenzione-e-il-contrasto-dei-crimini-informatici-s/index.html

di scaricare allegati o cliccare su link malevoli. Se il mittente è sconosciuto, è meglio evitare qualsiasi azione di apertura e procedere con l'eliminazione del messaggio; se il mittente è conosciuto, bisogna controllare la veridicità dell'invio, questo perché il mittente potrebbe avere la casella di posta infetta da un virus e, di conseguenza, infetterebbe anche il computer del destinatario.[32]

Un'ulteriore tecnica potrebbe essere quella di controllare gli accessi agli account social e impostare la privacy. Se un cyber-criminale entra in possesso degli accessi dell'account di un soggetto, potrebbe modificare le impostazioni e le informazioni, oppure utilizzare le immagini in maniera fraudolenta. Potrebbe inoltre cambiare i dati di accesso. È importante, poi, controllare la rete e la "normalità" del computer, questo perché alcuni attacchi causano danni evidenti e quindi è facile riconoscerli. Questa situazione spesso si configura quando viene cliccato un link infetto. Conviene sempre installare un antivirus che oltre a scansionare il computer, permette anche di analizzare l'affidabilità dei siti.[33]

Un ulteriore accorgimento da prendere in considerazione è la grammatica e l'ortografia: se una mail è ricca di errori grammaticali si può essere certi che si tratta di phishing; solitamente queste mail fraudolente vengono scritte in una lingua, per poi essere tradotte mediante traduttore automatico. Un altro chiaro segnale di phishing è la presenza di un modulo che richiede di inserire i propri dati via e-mail.[34]

Il compito di lottare contro queste tipologie di crimini spetta alla Polizia, ai Dipartimenti nazionali di sicurezza e alle aziende private attive nel settore, ma anche a livello personale è possibile mettere in atto degli accorgimenti volti a prevenire la proliferazione di tali attacchi. Ciò che è consigliato fare è installare nei dispositivi informatici un potente Antivirus; non cliccare su link presenti in email ricevute da mittenti sconosciuti; effettuare scansioni periodiche per analizzare il sistema e rimuovere i file pericolosi; evitare di scaricare file da

[32] ithesiasistemi.it/2017/07
[33] ivi
[34] ivi

fonti sconosciute; non fornire password o dati bancari; verificare la sicurezza di un sito prima di inserire le credenziali d'accesso; utilizzare password sicure ed efficaci.[35]

5. Soggetti attivi e responsabilità

Pur essendo i reati informatici reati comuni, le fattispecie incriminatrici fanno riferimento a soggetti di fatto in possesso di particolari qualità, sulla base dell'attività svolta o delle loro particolari competenze specifiche. In particolare, alcune norme indicano che colui che compie l'azione è il cosiddetto operatore di sistema, ossia colui che sorveglia o fa funzionare o fa funzionare un sistema informatico.[36]

In altri casi si fa riferimento alla figura del provider, che nella sua dicitura estesa è l'Internet Service Provider (ISP), nonché fornitore di servizi internet. Tale è ogni persona fisica, società o altro ente che fornisce a terzi l'accesso ad internet, gestendone la rete. Il provider viene detto access provider, quando si limita a fornire la sola connessione alla rete; esso non è generalmente ritenuto responsabile per gli illeciti che vengono realizzati da terzi utilizzando la rete da costui gestita. Viceversa, può incorrere in ipotesi di responsabilità, anche penali, il provider che non si limiti alla semplice fornitura di accesso alla rete, ma fornisca anche servizi ulteriori ed aggiuntivi, dal catching[37] all'hosting[38] (content provider).[39]

La responsabilità generalmente dipende alla circostanza che il provider sappia che l'attività o l'informazione trasmessa siano illecite. Il provider è, quindi, responsabile dell'illecito posto in essere dall'utilizzatore allorché egli abbia piena consapevolezza del carattere antigiuridico dell'attività svolta da quest'ultimo. Tale responsabilità si configura, quindi, al pari di una responsabilità soggettiva: colposa, allorché il fornitore del servizio, consapevole della

[35] Unicusano.it
[36] https://www.bptmavvocati.it/portfolio/i-soggetti-attivi-nei-reati-informatici/
[37] Per svolgere tale attività il motore di ricerca procede a eseguire una copia di ogni sito che viene memorizzata temporaneamente in una cache, attività che consente di fornire per le chiavi di ricerca più frequentemente utilizzate i risultati della ricerca stessa in tempi estremamente rapidi
[38] L'allocazione delle pagine di un sito o di un'applicazione web su un server web, ciò permette al sito o all'applicazione di essere raggiungibili e visibili agli utenti in rete.
[39] https://www.bptmavvocati.it/portfolio/i-soggetti-attivi-nei-reati-informatici/

presenza sul sito di materiale sospetto, si astenga dall'accertarne l'illiceità e, al tempo stesso, dal rimuoverlo; dolosa, quando egli sia consapevole anche dell'antigiuridicità della condotta dell'utente e, ancora una volta, ometta di intervenire.[40]

6. Prevenzione nel d.lgs. 231/2001

Con l'adozione del decreto 231/2001 viene sancita definitivamente la responsabilità delle aziende nel caso di reati portati a compimento dal personale interno. Quindi, anche laddove non si conosca l'identità del possibile autore (persona fisica), la persona giuridica all'interno della quale si è verificato il fatto di reato, può ritenersi responsabile laddove si verificano lacune nell'organizzazione o venga individuato l'elemento dell'interesse o vantaggio.[41]

Il primo passo da affrontare è quello di predisporre un Modello Organizzativo, tenendo conto delle specificità del singolo ente. Il Modello Organizzativo (MOG), consiste in un insieme di norme, principi e regole volto a prevenire la proliferazione dei reati informatici commessi non solo ai danni dell'azienda, ma anche all'interno della stessa. Tale MOG dovrà anticipare le sedi, le modalità e le finalità del compimento dei reati d'impresa, in modo da eseguire dei controlli volti a garantire la massima trasparenza alle varie operazioni informatiche, sia svolte a livello apicale, sia tra i dipendenti.

Al fine di evitare il rischio di accessi anomali mirati a danneggiare o sottrarre i dati in possesso dei dipendenti, è importante adottare un regolamento relativo all'utilizzo delle risorse informatiche aziendali e le procedure in materia di sicurezza; definire formali requisiti di autenticazione; procedere ad una verifica periodica dei sistemi di accesso e definire le modalità di definizione delle password, per accordare o revocare l'accesso ai sistemi informativi. [42]

---

[40] ivi

[41] L. LUPARIA, Cybercrime e responsabilità degli enti. A cura di Luca Luparia, Varese, Giuffrè editore, 2009, p. 96

[42] ornarieassociati.com/focus-cybercrimes-e-responsabilita-da-reato-degli-enti-rischi-penali-e-prevenzione/

Al fine di evitare il rischio di accessi anomali mirati a danneggiare o sottrarre i dati in possesso dei dipendenti, è importante adottare un regolamento relativo all'utilizzo delle risorse informatiche aziendali e le procedure in materia di sicurezza; definire formali requisiti di autenticazione; procedere ad una verifica periodica dei sistemi di accesso e definire le modalità di definizione delle password, per accordare o revocare l'accesso ai sistemi informatici. [43]

[43] ornarieassociati.com/focus-cybercrimes-e-responsabilita-da-reato-degli-enti-rischi-penali-e-prevenzione/

CAPITOLO 3

REPRESSIONE DEI REATI INFORMATICI

1. La denuncia di un crimine informatico

Per denunciare un crimine informatico in Italia, è necessario rivolgersi alla Polizia Postale, ovvero il corpo a cui competono le indagini sui crimini informatici. In caso di denuncia, la Polizia Postale effettuerà le indagini necessarie per individuare i responsabili e raccogliere le prove del reato commesso. L'organismo è strutturato in vari dipartimenti specializzati per ogni specifico reato.

La denuncia può essere presentata presso una qualsiasi Questura o Commissariato di Polizia locale, oppure può essere fatta online attraverso il sito web della Polizia di Stato. È importante fornire tutte le informazioni disponibili sui reati di cui si è vittime, inclusi, se conosciuti, i dati del responsabile e le eventuali prove a supporto della denuncia.

Una volta presentata la denuncia *online*, il sistema rilascerà una ricevuta elettronica e un numero di protocollo che serviranno per recuperare la pratica dal vivo, ovvero recandosi presso l'ufficio della Polizia di Stato preposto. La denuncia presentata online assume valore legale soltanto nel momento in cui viene sottoscritta davanti all'ufficiale di polizia giudiziaria; rimane comunque una possibilità per segnalare, il prima possibile, l'esistenza di un crimine.[44]

È anche possibile segnalare la commissione di un reato informatico ad un soggetto diverso. Si allude al provider, il quale, una volta messo a conoscenza della commissione di un illecito online, ha la responsabilità di rimuovere i contenuti che presentano questa connotazione. Proprio per tale motivo, i provider più conosciuti mettono a disposizione un indirizzo di posta elettronica per segnalare gli abusi.

[44] https://www.dequo.it/

2. La Polizia Postale e la sua organizzazione

Il Servizio centrale delle Polizia Postale e delle Comunicazioni ha sede a Roma e coordina 20 compartimenti regionali e 80 sezioni territoriali. Un'organizzazione che permette una presenza diffusa su tutto il territorio nazionale grazie alla presenza di circa duemila uomini e donne del Dipartimento di Pubblica Sicurezza che mettono a disposizione le loro qualifiche professionali, le conoscenze informatiche e le loro esperienze di polizia giudiziaria.[45]

A causa dell'assenza di confini e dell'articolata distribuzione di Internet le forze di polizia dei singoli Paesi devono garantire una presenza capillare non solo sul territorio nazionale, ma anche una collaborazione a livello internazionale che assicura la perseguibilità dell'autore di un eventuale reato commesso attraverso la rete.

Il pilastro fondamentale della divisione operativa è la sezione dedicata alle collaborazioni internazionali impegnata con omologhi Uffici di Polizia stranieri nel contrasto al Cybercrime.

Accanto alla Polizia Postale vi è l'U.A.C.I. (Unità di analisi sul crimine informatico – *Computer Crime Analysis Unit*), la quale funzione è quella di affiancare gli investigatori della Polizia Postale e delle Comunicazioni nelle indagini sui crimini ad alta tecnologia, progettando nuove tecniche investigative e tracciando profili psicologici e comportamentali degli autori di tali crimini.

Le attività principali della struttura consistono in ricerche e studi sul fenomeno della criminalità informatica in collaborazione con Università, Aziende ed Istituzioni; sperimentazione di nuove tecniche investigative in materia di computer crime; progettazione di percorsi di formazione sulla sicurezza informatica e computer crime in collaborazione con Università e aziende; divulgazione di informazioni e risultati di ricerche in contesti scientifici; assistenza psicologica degli investigatori che si occupano di computer crime (pedofilia).[46]

---

[45] https://www.commissariatodips.it/profilo/attivita-e-organizzazione/index.html
[46] https://www.commissariatodips.it/profilo/unita-di-analisi-sul-crimine/index.html

3. Come agisce la Polizia Postale?

La Polizia Postale dispone di una vasta gamma di mezzi per indagare sui reati informatici; uno dei principali strumenti utilizzati è la *Digital Forensics*, che si occupa della raccolta, conservazione, analisi e presentazione delle prove digitali in caso di reati informatici. Consiste in uno strumento cruciale per la risoluzione dei crimini informatici, non solo perché permette di raccogliere prove, ma anche per consentire la difesa degli imputati, consentendo loro di dimostrare la propria innocenza.

Gli esperti raccolgono gli elementi di prova con metodologie scientifiche e adeguate procedure per preservare l'integrità dei dati, che poi vengono analizzati ed interpretati utilizzando strumenti e software specifici.

La Polizia Postale può anche utilizzare, su autorizzazione dell'autorità giudiziaria, strumenti come le intercettazioni, la geolocalizzazione e l'analisi dei dati, per individuare i soggetti coinvolti. Inoltre può collaborare con altre agenzie governative o organizzazioni internazionali per condividere informazioni e coordinare le indagini.[47]

4. L'individuazione del giudice competente

Un aspetto particolarmente problematico riguarda l'individuazione del giudice territorialmente competente per un reato informatico. Secondo la giurisprudenza, viene considerato come luogo di commissione del reato quello in cui si trova la piattaforma in cui ha operato il cliente, quindi il luogo in cui si trova il server che ha elaborato le credenziali del soggetto criminale.

Ove non sia possibile rintracciare il luogo in cui si trova la piattaforma in cui ha operato il cliente, si applicano le regole suppletive stabilite dall'articolo 9 c.p.p.:

- Il giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione;

[47] https://www.cisbroker.it/n/47-crimini-informatici-come-fare-denuncia-e-come-agisce-la-polizia-postale.html

- Il giudice della residenza, della dimora o del domicilio dell'imputato;
- Il giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato.

5. Come vengono puniti i reati informatici?

Le pene previste per i reati informatici sono molto pesanti. L'intento del legislatore è quello di fare in modo che un soggetto non commetta più lo stesso reato o, più in generale, evitare il compimento di quel determinato fatto di reato.

Vediamo ora le varie pene che vengono irrogate a ciascun soggetto autore di un reato informatico:

- Intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche senza autorizzazione: la pena consiste nella reclusione che può variare da un anno e sei mesi fino a cinque anni; la pena può, invece, essere da tre ad otto anni se il fatto è stato commesso in danno ad un sistema informatico o telematico utilizzato dallo Stato o da un altro ente pubblico; da un pubblico ufficiale o da un da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri; da chi esercita anche abusivamente la professione di investigatore privato;

- Detenzione e diffusione abusiva di codici di accesso al sistema: la pena consiste nella reclusione sino a due anni e con la multa sino a euro 5.164;

- Diffusione di hardware e software diretti a danneggiare il sistema: la pena consiste nella reclusione fino a due anni e con la multa sino a euro 10.329;

- Accesso abusivo ad un sistema informatico: la pena consiste nella reclusione fino a tre anni. Nel caso in cui 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; il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 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, la pena è della reclusione da uno a cinque anni;

- Frode informatica: la pena consiste nella reclusione da sei mesi a tre anni e con la multa da euro 51 a 1.032; oppure la reclusione può essere da due a sei anni e la 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.

CAPITOLO 4

I REATI INFORMATICI A LIVELLO EUROPEO E NEL MONDO

1. L'a-territorialità

Le caratteristiche di transnazionalità[48] e immaterialità della rete comportano che i reati commessi attraverso Internet siano molto più difficili da perseguire, perché non solo la rete viene considerata uno spazio libero, ma anche perché, a differenza dei reati comuni, in cui luogo, persone e cose sono facilmente individuabili, i reati informatici vengono consumati in luoghi virtuali e hanno per oggetto beni intangibili. Rispetto ad un criminale comune, l'autore di un reato informatico ha la possibilità di poter compiere il fatto di reato da uno Stato estero, utilizzando un dispositivo all'estero ed impiegare un flusso di rete che attraversa reti estere.

In questi casi, quando viene compiuto un fatto all'estero, le autorità per eseguire le indagini e acquisire informazioni relative ad un reato devono ottenere autorizzazioni e affrontare diverse ostacoli processuali.

Le legislazioni dei vari Stati sono diverse e disomogenee. È quindi necessario intervenire creando una normativa comune per risolvere i problemi che derivano dalla transnazionalità di questi reati.

[48] Un reato è di natura transnazionale qualora sia commesso in più di uno Stato, o sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato, o sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato, ovvero sia commesso in uno Stato ma produca effetti sostanziali in un altro Stato.

2. Un quadro europeo

In territorio europeo, il primo Consiglio d'Europa dedicato ai reati legati all'uso delle tecnologie informatiche è avvenuto nel 1999 a Tampere (Finlandia). La consapevolezza della rilevanza internazionale del cybercrime, si è concretizzata con l'approvazione della Convenzione di Budapest, firmata il 23 novembre 2001. Tale Convenzione rappresenta il primo accordo internazionale sui reati commessi tramite Internet. La firma del Trattato viene lasciata agli Stati membri e non membri che hanno partecipato alla stesura, ma è aperta anche agli Stati non membri che non sono intervenuti.

Tale convenzione ha imposto a tutti gli Stati presenti al Consiglio d'Europa "di adottare misure legislative rivolte alla repressione penale dei nuovi crimini informatici, armonizzando in questo modo i diversi ordinamenti giuridici interni e coordinando forme di collaborazione per quanto concerne la raccolta di prove da parte delle autorità."[49]

Il trattato è composto da 48 articoli, suddivisi in quattro capitoli. Il primo capitolo contiene alcune definizioni, come quella di "sistema informatico", di "dati informatici", di "service provider" e di "trasmissione di dati". Il secondo capitolo è il fulcro del trattato in quando definisce i provvedimenti da adottare a livello nazionale; il terzo capitolo riguarda, invece, la cooperazione internazionale.

Alla Convenzione di Budapest hanno presenziato sia Stati europei che Stati non membri; inizialmente, avevano aderito 47 Stati. Tra questi, 7 Stati hanno aderito ma alla firma non è seguita nessuna ratifica. Gli Stati europei che non hanno né firmato né ratificato sono San Marino e la Russia. Successivamente altri stati hanno aderito alla Convenzione, come gli Stati Uniti d'America e l'Italia che ha aderito con la Legge n. 48 del 2008, aggiornando le disposizioni della legge 547/1993.

Per quanto riguarda il diritto internazionale, il principio di stretta territorialità cede il posto a quello di ultraterritorialià[50]. Ciò potrebbe essere un elemento di notevole rilevanza per

[49] https://amslaurea.unibo.it/9489/4/Tesi_-_Laura_Conti.pdf
[50] Piccinni MarioLeone, Vaciago Giuseppe, "Computer Crimes – Casi pratici e metodologie investigative dei reati informatici", pag.67, 2008

scoraggiare i criminali informatici, i quali agiscono con la convinzione di non poter essere sanzionati grazie all'applicazione del principio di territorialità. Per fronteggiare la "globalizzazione del crimine" si mira a realizzare una "globalizzazione della giustizia", in modo tale da consentire alle autorità di reprimere la criminalità informatica transnazionale.[51]

3. Un quadro extraeuropeo

La minaccia della criminalità informatica sulla sicurezza economica, politica e sugli interessi pubblici sta iniziando sempre più ad essere presa in considerazione sia dai Governi dei paesi sviluppati, sia dai Governi dei paesi che sono attualmente in via di sviluppo. Molte organizzazioni hanno già provveduto, e altre stanno già provvedendo, a stabilire regole a livello regionale e internazionale. Un chiaro esempio possiamo notarlo con la cooperazione tra Stati Uniti e Cina, due paesi in cui la criminalità informatica è sviluppata ai massimi livelli. Infatti, nel gennaio 2011, i due Stati hanno collaborato su base bilaterale in tema di sicurezza informatica, stabilendo un approccio denominato "Fighting Spam to Build Trust"[52].[53]

Nel 1997 il G8, ossia un gruppo informale che riunisce annualmente i capi di Stato e di Governo delle maggiori democrazie industriali (Canada, Francia, Gran Bretagna, Germania, Giappone, Italia, Russia e Stati Uniti) in accordo con l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) affiancati dal Fondo Monetario Internazionale (FMI), dalla Banca Mondiale (BM) e dall'Organizzazione Mondiale del Commercio (WTO)[54], rilasciò un comunicato che prevede un piano d'azione per contrastare il cybercrime e proteggere i dati e i sistemi da accessi non autorizzati; inoltre invita gli Stati membri ad accordare un punto di unione fra essi.

[51] https://amslaurea.unibo.it/9489/4/Tesi_-_Laura_Conti.pdf
[52] Traduzione: combattere lo spam per creare fiducia.
[53] https://www.chinafile.com/Fighting-Spam-Build-Trust
[54] https://www.edscuola.it/archivio/interlinea/gotto.html

È intervenuta, poi, l'Assemblea Generale delle Nazioni Unite, la quale ha adottato due risoluzioni contro l'abuso criminale delle tecnologie dell'informazione; all'interno delle Nazioni Unite vi è un'agenzia specializzata, denominata "International Telecommunication Unit" (ITU) che detiene un ruolo primario nella sicurezza informatica. [55]

Come si è avuto modo di vedere, tutto il mondo è interconnesso e tutti i settori vitali dell'economia e della società dipendono altamente dall'uso dei computer e della rete Internet [56]. "Cyber space is their nervous system – the control system of our country. Cyber space is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work.[57]"[58]

[55] https://www.itu.int/en/Pages/default.aspx

[56] Un esempio di cybercrime che è avvenuto negli Stati Uniti ma che ha avuto ripercussioni anche in alcuni Stati presenti in Europa è il caso in cui uno studente delle Filippine, nel 2001, ha rilasciato un virus denominato "*I love You*", infettando e isolando i computers della Casa Bianca, del Pentagono e dell'FBI. Tale virus però ha prodotto danni anche in Europa, infettando i sistemi del Parlamento inglese, danese e del governo federale della Svizzera (https://www.corriere.it/tecnologia/20_maggio_04/i-love-you-venti-anni-fa-primo-virus-informatico-che-ha-messo-mondo-ginocchio-71e8565a-8dda-11ea-b08e-d2743999949b.shtml)

[57] Il cyberspazio è il loro sistema nervoso, il sistema di controllo del nostro Paese. Il cyberspazio è composto da centinaia di migliaia di computer, server, router, switch e cavi in fibra ottica interconnessi che consentono il funzionamento delle nostre infrastrutture critiche.

[58] https://www.dhs.gov/xlibrary/assets/nipp_it.pdf

CONCLUSIONE

L'utilizzo sempre più diffuso di strumenti digitali nella nostra quotidianità ha prodotto un notevole aumento dei reati commessi in rete. Ci si trova a fronteggiare casi di frode online, attività volte a danneggiare sistemi informatici e telematici, accessi abusivi a sistemi informatici e furto d'identità.

Il rischio di essere vittima di un crimine informatico è particolarmente elevato, soprattutto nell'ipotesi in cui l'utente non faccia un uso consapevole dei dispositivi digitali.

Non è un caso che negli ultimi tempi le vittime di reati informatici sono aumentate in modo esponenziale. Si ritiene quindi fondamentale intervenire sia sul piano della prevenzione, informando gli utenti dei rischi nei quali potrebbero incorrere e promuovendo l'adozione di modelli organizzativi nelle imprese, sia su quello repressivo, inasprendo le pene previste per tale forma di criminalità.

BIBLIOGRAFIA

Luca Luparia, *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008 n. 48)*, Milano, Giuffrè Editore, 2009.

Andrea Monti, *Cybercime e responsabilità da reato degli enti. Prevenzione, modello organizzativo e indagini preliminari*, Milano, Giuffrè Francis Lefevbre, 2022

Vania Contraffatto, *I reati informatici*, Frosinone, Key Editore, 2017

Piccinni MarioLeone, Vaciago Giuseppe, *Computer Crimes – Casi pratici e metodologie investigative dei reati informatici*. Moretti Honegger, 2008

SITOGRAFIA

https://www.sergentelorusso.it/cosa-e-la-digitalizzazione-vantaggi-come-iniziare/

https://universeit.blog/digitalizzazione/

https://www.riskmanagement360.it/cybersecurity/sicurezza-informatica-e-d-lgs-231-come-proteggersi-dalla-responsabilita-penale/

https://www.weclapp.it/glossario/digitalizzazione/

https://servicematica.com/la-catastrofe-dellinformazione-nel-futuro-il-nostro-corpo-sara-fatto-di-bit/

https://www.leurispes.it/la-digitalizzazione-della-vita-quotidiana/

https://digitale.moondo.info/breve-storia-della-digitalizzazione/

https://giurisprudenza.unipg.it/files/generale/Laboratorio_inf/reatiinformatici.pdf

https://www.phersei.com/cybersecurity/reati-informatici

https://www.procura.milano.giustizia.it/reati-informatici.html

https://it.wikipedia.org/wiki/Crimine_informatico

https://www.altalex.com/documents/news/2013/09/20/d-lgs-231-2001-responsabilita-amministrativa-da-reato

https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2001-06-08;231!vig=

https://www.csigbologna.it/referenze/giurisprudenza/la-legge-48-2008-a-dieci-anni-dalla-pubblicazione/#:~:text=La%20Legge%2048%2F2008%3A%20da%20dove%20partiva&text=547%20del%201993%20che%20aveva,mezzi%20di%20ricerca%20della%20prova.

https://www.riskmanagement360.it/compliance/il-modello-di-organizzazione-e-gestione-del-d-lgs-231-2001-struttura-e-caratteristiche/

https://www.telsy.com/it/cybersecurity-e-prevenzione-dei-reati-informatici-ai-sensi-del-d-lgs-231-2001/

https://www.4clegal.com/opinioni/delitti-informatici-dlgs-23101-violazione-dati-punti-contatto-due-normative

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1607859

https://www.cybersecurity360.it/nuove-minacce/reati-informatici-e-d-lgs-231-2001-fattispecie-sanzioni-e-soluzioni-preventive/

https://www.rivista231.it/Legge231/Pagina.asp?Id=718

https://www.aodv231.it/documenti-di-approfondimento/la-prevenzione-dei-reati-informatici-rischi-231-data-protection-e-misure-di-compliance-giugno-23/

https://studiolegaleramelli.it/2021/03/01/i-reati-informatici-e-commessi-a-mezzo-strumenti-informatici-previsti-e-puniti-dal-codice-penale-e-dalla-legge-sulla-protezione-del-diritto-dautore-corredati-con-la-rassegna-di-giurisprudenza/

https://it.linkedin.com/pulse/modello-231-come-prevenire-i-reati-informatici-davide-leonardi

https://www.diritto.it/wp-content/uploads/old2022/archivio/1/26626.pdf

http://www.interlex.it/testi/l547_93.htm#:~:text=%2DChiunque%20commette%20un%20fatto%20diretto,da%20uno%20a%20quattro%20anni.

https://www.studiocuomo.it/reati-informatici/

https://www.sixtema.it/digital-transformation/data-protection-e-cyber-security/cybercrime-definizione-e-tipologie/#:~:text=utilizzo%20della%20tecnologia%20informatica%20per,'abuso%3A%20spam%2C%20malware%3B&text=utilizzo%20della%20tecnologia%20informatica%20nella,identit%C3%A0%2C%20Information%20warfare%2C%20phishing.

https://www.aodv231.it/images/atti/1201-10 Sanzioni%20interdittive_%20sicurezza%20sul%20lavoro.pdf

https://fornarieassociati.com/focus-cybercrimes-e-responsabilita-da-reato-degli-enti-rischi-penali-e-prevenzione/

https://www.ey.com/it_it/technology/cybersecurity-compliance

https://www.sergentelorusso.it/cosa-e-la-digitalizzazione-vantaggi-come-iniziare/

https://www.pandasecurity.com/it/mediacenter/sicurezza/reati-informatici-quali-sono/

https://www.unicusano.it/blog/universita/crimine-informatico/

https://archiviodpc.dirittopenaleuomo.org/d/6549-un-possibile-principio-di-risposta-legislativa-alle-domande-concernenti-la-dignita-nella-fase-final

https://www.onoratoinformatica.it/sicurezza-cibernetica/i-5-reati-informatici-quali-sono/

https://www.carabinieri.it/in-vostro-aiuto/consigli/internet/i-crimini-informatici

https://www.procura.milano.giustizia.it/reati-informatici.html

https://www.aodv231.it/catalogo-reati/intercettazione--impedimento-o-interruzione-illecita-di-comunicazioni-informatiche-o-telematiche--art--617-quater-c-

p/#:~:text=o%20telematiche%20(art.-,617%2Dquater%20c.p.)%20%5Barticolo%20modificato%20dalla%20Legge%20n.,sei%20mesi%20a%20cinque%20anni.

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-v/art617quater.html

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-v/art617quinquies.html?utm_source=internal&utm_medium=link&utm_campaign=articolo&utm_content=nav_art_succ_dispositivo

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-v/art617sexies.html?utm_source=internal&utm_medium=link&utm_campaign=articolo&utm_content=nav_art_succ_dispositivo

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-v/art617septies.html?utm_source=internal&utm_medium=link&utm_campaign=articolo&utm_content=nav_art_succ_dispositivo

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iv/art615quinquies.html

https://www.dogma.it/it/news/cos-e-un-virus-trojan-e-come-funziona

https://it.wikipedia.org/wiki/Trojan_(informatica)

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xiii/capo-ii/art640ter.html

https://www.google.com/search?q=dialer+cos%27%C3%A8&oq=dialer+cos%27%C3%A8&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIICAEQABgWGB4yCAgCEAAYFhgeMggIAxAAGBYYHjIICAQQABgWGB4yCAgFEAAYFhgeMggIBhAAGBYYHjIICAcQABgWGB4yCAgIEAAYFhge0gEINDA2N2owajSoAgCwAgA&sourceid=chrome&ie=UTF-8

https://assistenza-legale-imprese.it/d-lgs-n-231-2001-responsabilita-enti/

https://www.smartius.it/data-it-law/guida-reati-informatici-azienda/reati-informatici-dipendente-responsabile-datore-lavoro/

https://www.google.com/search?q=attacchi+ransomware&oq=attacchi+ramso&gs_lcrp=EgZjaHJvbWUqCggBEAAYChgWGB4yBggAEEUYOTIKCAEQABgKGBYYHtIBCDM5MDRqMGo0qAIAsAIA&sourceid=chrome&ie=UTF-8

https://www.fog.it/corsoinformatica/reati.htm#:~:text=547%2F93%2C%20prevede%20che%20la,un%20sistema%20informatico%20o%20telematico.

https://www.commissariatodips.it/profilo/cnaipic/index.html#:~:text=Cnaipc%20Il%20C.N.A.I.P.I.C.,critica%20e%20di%20rilevanza%20nazionale.

https://www.commissariatodips.it/notizie/articolo/polizia-di-stato-e-anci-siglano-laccordo-sulla-prevenzione-e-il-contrasto-dei-crimini-informatici-s/index.html

https://www.cybersecurity360.it/cultura-cyber/reati-informatici-quali-sono-e-che-cosa-si-rischia/

https://www.ithesiasistemi.it/2017/07/6-modi-rilevare-ed-evitare-un-attacco-informatico/

https://www.cybertrends.it/10-tipi-di-cybercrime-come-proteggersi/

https://www.alteredu.it/reati-informatici-cosa-sono-cosa-sapere/

https://www.key4biz.it/crimini-informatici-accordo-regione-lepida-e-polizia-postale-su-prevenzione-e-contrasto/455939/

https://www.interno.gov.it/it/temi/sicurezza/crimine-informatico/centro-nazionale-anticrimine-informatico-protezione-infrastrutture-critiche-cnaipic

https://www.unifi.it/art-6669-prevenzione-e-contrasto-dei-crimini-informatici-sui-sistemi-informativi.html

https://www.diritto.it/la-responsabilita-amministrativa-degli-enti-i-reati-informatici/

https://www.bptmavvocati.it/portfolio/i-soggetti-attivi-nei-reati-informatici/

https://boglione.eu/approfondimento/responsabilita-dellhosting-provider-e-catching

https://www.miur.gov.it/bullismo-e-cyberbullismo

https://www.generazioniconnesse.it/site/it/0000/00/00/pedopornografia-online/

https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-ii/art595.html

https://www.consulenzalegaleitalia.it/diffamazione/#:~:text=La%20diffamazione%20%C3%A8%20un%20reato,mediante%20comunicazione%20con%20pi%C3%B9%20persone.

https://www.poliziadistato.it/articolo/385d66573e97fe4751254032

https://www.cisbroker.it/n/47-crimini-informatici-come-fare-denuncia-e-come-agisce-la-polizia-postale.html

https://www.dequo.it/articoli/polizia-postale-reati-informatici#1-polizia-postale-denuncia-e-segnalazioni-

https://www.studiolegaledelalla.it/cose_da_sapere/reati-informatici-ingiuria-2/

https://www.trenodoc.it/reati-informatici-ecco-cosa-sono-e-come-vengono-puniti/#:~:text=in%20pi%C3%B9%2C%20il%20codice%20penale,arrivare%20fino%20a%20tre%20anni.

https://legalfordigital.it/reati-informatici/reati-informatici-quali-sono/

https://www.commissariatodips.it/profilo/unita-di-analisi-sul-crimine/index.html

https://www.laleggepertutti.it/634523_cosa-succede-quando-si-fa-una-denuncia-alla-polizia-postale

https://www.commissariatodips.it/approfondimenti/approfondimenti-generali/la-denuncia-di-privati/index.html

https://vitolavecchia.altervista.org/quali-sono-e-come-contrastare-i-reati-informatici-piu-diffusi/

https://avvocato-penalista.milano.it/avvocato-reati-informatici/#:~:text=ad%20euro%2010.329.-,Il%20reato%20di%20detenzione%20e%20diffusione%20abusiva%20di%20codici%20di,multa%20fino%20ad%20euro%205.164.

https://appuntieconsigli.wixsite.com/appuntieconsigli/pena#:~:text=La%20pena%20%C3%A8%20la%20sanzione,pu%C3%B2%20definire%20quindi%20come%20la

https://www.commissariatodips.it/profilo/collaborazione-internazionale/index.html

https://www.corriere.it/tecnologia/20_maggio_04/i-love-you-venti-anni-fa-primo-virus-informatico-che-ha-messo-mondo-ginocchio-71e8565a-8dda-11ea-b08e-d2743999949b.shtml

https://www.dhs.gov/xlibrary/assets/nipp_it.pdf

https://www.chinafile.com/Fighting-Spam-Build-Trust

https://www.edscuola.it/archivio/interlinea/gotto.html