Progetto SICUREZZA

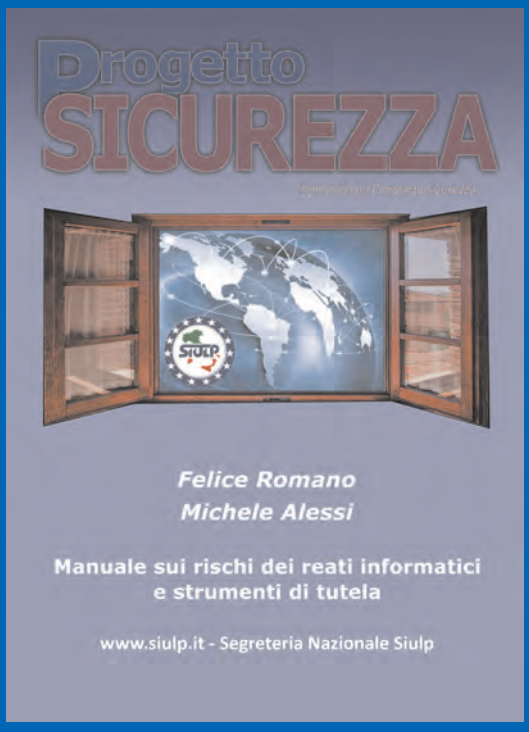
il mensile del Comparto sicurezza

Felice Romano

Michele Alessi

Manuale sui rischi dei reati informatici e strumenti di tutela

www.siulp.it - Segreteria Nazionale Siulp



Progetto SICUREZZA

Il mensile del Comparto sicurezza

Periodico mensile ufficiale del
Sindacato Italiano Unitario Lavoratori Polizia

Anno XXVI n. 1/2014 - € 2,58

Proprietà della testata: Siulp

Direttore politico responsabile
Felice Romano

Comitato di redazione
Michele Alessi, Innocente Carbone
Vittorio Costantini,Antonio Lanzilli
Alessandro Pisaniello
Primo Sardi

Tiratura
Copie stampate: 58.000
Distribuite in abbonamento: 45.000

Registrazione
Tribunale di Roma nr. 54/88 del 27/01/1988
iscrizione al ROC n. 1123

Edito da
Siulp

Direzione, redazione e amministrazione
Via Vicenza 26, 00185 Roma
Tel.: 06.4455213 - Fax: 06.4469841
nazionale@siulp.it - www.siulp.it

Abbonamenti ordinari
Appartenenti alle Forze di Polizia
e Vigili Urbani € 19,63
Pensionati delle forze di Polizia € 12,91

Progetto grafico e stampa a cura di
reproSTAMPA s.r.l.
TIPOLITOGRAFIA
00148 Roma - Via Cesare Dal Fabbro, 15
Tel.: 06.6557765 - Fax: 06.65678177
e-mail: info@reprostampa.com

"Con tono giusto si può dire tutto.
Con tono sbagliato nulla.
L'unica difficoltà consiste
nel trovare il tono".

George Bernard Shaw

INDICE

PREFAZIONE

di Gianpiero Gamaleri

Professore ordinario di Sociologia della comunicazione, Preside della Facoltà di Scienze della comunicazione, Università Telematica Internazionale Uninettuno di Roma, già membro del C.d.A della Rai, Socio Onorario del SIULP

UNA POLIZIA DI STATO PROIETTATA NEL FUTURO DIGITALE PER REPRIMERE I REATI INFORMATICI E PER GUIDARE IL CAMBIAMENTO VERSO OBIETTIVI DI CRESCITA CIVILE, INDIVIDUALE E COLLETTIVA

Questo manuale fa onore a un sindacato – qual'è il SIULP – che non si limita alla giusta difesa dei diritti degli iscritti, ma vuole partecipare a pieno titolo anche allo sviluppo presente e futuro delle attività della Polizia di Stato, condividendo e anticipando le profonde trasformazioni che investono l'intera società e in particolare il settore della sicurezza.

E non è un caso che sia stato personalmente curato dai vertici del sindacato, il Segretario Generale Nazionale Felice Romano e il Segretario Nazionale Michele Alessi.

Chi opera in questo campo ai massimi livelli di responsabilità e di rappresentanza si trova infatti in prima linea nel cogliere la straordinaria evoluzione che sta attraversando il nostro sistema sociale. Non si tratta solo di teorie del cambiamento o di racconti di fantascienza, ma di un'effettiva, profonda e rapida modificazione delle relazioni sociali e interpersonali quale l'umanità non ha mai affrontato nei secoli precedenti.

Uno studioso ha scritto recentemente una frase lapidaria: "Il mondo intero si sta

trasformando in informazione". Con ciò intendendo che non esiste più relazione umana, pubblica o privata, che non sia investita, per così dire, dallo "tsunami digitale". Pensiamo ai grandi eventi pubblici, inevitabilmente esposti alle comunicazioni radiotelevisive satellitari. Pensiamo alle relazioni personali, anche dei più piccoli, ormai veicolate all'interno dei circuiti dei cellulari, degli i-phone, dei siti web, dei contatti Skype e di tutti i linguaggi dei social network.

Una trasformazione prodigiosa, tutt'altro che esaurita, destinata anzi a dilatarsi enormemente anche nel prossimo futuro (ogni sei mesi c'è una grande novità planetaria, il lancio di nuove applicazioni), che porta con sé eccezionali possibilità, ma anche insidie che devono essere ben individuate e represse.

RENDERE SICURO IL "MONDO UNO", RENDERE PRATICABILE SENZA RISCHI IL "MONDO DUE"

Per descrivere la portata di questa colossale trasformazione, potremmo ricorrere a un'immagine quanto mai efficace. Nel giro di pochi decenni, il mondo della realtà fisica, della nostra vita quotidiana è stato, per così dire, avvolto da una sfera più ampia che investe ormai tutto il pianeta, dalle più ampie realtà politiche e istituzionali (pensiamo alle attività di governo) fino alle relazioni più piccole, minute, quelle che intercorrono tra i singoli cittadini, compresi i più deboli e indifesi verso cui va sempre l'attenzione di chi deve garantirne la sicurezza.

E' stato osservato, giustamente, che il **"mondo uno",** quello delle nostre relazioni concrete e reali, è stato circondato da un **"mondo due",** quello delle relazioni virtuali: un mondo digitale che non si limita a riprodurre quello reale, ma impone proprie regole e procedure che assumono un loro dinamismo e spesso sfuggono ai tentativi di controllo di quanti vi si avventurano e persino di coloro che le hanno create.

Pensiamo soltanto a quello che è stato chiamato **il diritto all'oblio**, cioè il diritto a ricominciare, a far dimenticare alcuni sbagli che possono aver avuto non solo una rilevanza penale, ma anche una semplice ma dolorosa perdita di reputazione. Nel "mondo uno", quello reale, l'orientamento previsto anche nella nostra Carta Costituzionale è quello del ravvedimento e del recupero. Nel "mondo due", quello virtuale, certi sbagli o semplici leggerezze vengono conservate permanentemente, compromettendo l'immagine di un soggetto vita naturale durante.

E' frequente il caso di giovani, soprattutto ragazze, che imprudentemente mettono in rete proprie immagini intime, solo per un gioco tra amici, e poi non possono più recuperarle, non possono cancellarle perché ormai il sistema virtuale se ne è impossessato. E questo può dar luogo sia a una serie di traumi personali, sia anche alla commissione di reati, primo fra tutti la violazione delle privacy, quando non si arriva a vere e proprie forme di ricatto.

Tema questo attualissimo, infatti è di questi giorni la notizia che i gestori del famoso motore di ricerca internazionale "Google" hanno predisposto una pagina internet attraverso la quale chiunque può chiedere la cancellazione definitiva dei propri dati personali presenti nelle pagine e nei link trovati attraverso lo stesso motore di ricerca anche se pubblicati da terzi soggetti. Si riporta qui di seguito il link per il collegamento con il sito:

"https://support.google.com/legal/contact/lr_eudpa?product=websearch".

Già nei primi giorni da quando la pagina è stata messa on-line l'iniziativa ha suscitato un grandissimo interesse da parte degli internauti. Forse il "**mondo due**", quello virtuale, sta influenzando così tanto il mondo reale da diventarne

parte determinante nella sfera soggettiva, a tal punto che gli interessati cercano di intervenire prima che le loro informazioni personali vengano utilizzate per fini diversi da quelli realmente voluti, sfidando una realtà apparentemente familiare ed utile ma che si può trasformare in un incubo dai contorni più svariati . È da dire però che il merito dell'ottima iniziativa è della Corte di Giustizia europea che è intervenuta tempestivamente sul cosiddetto "**diritto all'oblio",** attraverso la Sentenza della Corte di Giustizia Europea del 13 maggio 2014 (Causa C-131/12), costringendo quindi i gestori di Google a redigere la pagina internet predetta al fine di tutelare la privacy di tutti i cittadini europei, ritenendo che "il gestore di un motore di ricerca su Internet è responsabile del trattamento effettuato dei dati personali che appaiono su pagine web pubblicate da terzi".

Altrettanto gravi sono i casi di **cyberbullismo** e ludopatia. Quelli che prima erano scherzi pur deprecabili, ma che si esaurivano tra le mura di una classe o di un ambiente scolastico, oggi viaggiano sul web e portano spesso alla disperazione i soggetti che ne sono vittime. L'intervento del docente o del genitore diventa vano quando certe immagini travalicano i confini di una scuola e sforano nell'ambiente virtuale del web dove ognuno vi può accedere, e spesso vi accedono proprio coloro da cui il soggetto non vorrebbe mai essere visto nelle condizioni rappresentate. Perchè il cyberbullismo assume diverse connotazioni quali la pubblicazione *on-line* di informazioni spiacevoli ed imbarazzanti su un'altra persona; l'estromissione deliberata di una persona da un gruppo *on-line* allo scopo di pregiudicare la sua sensibilità; l'invio reiterato di messaggi offensivi diretti a ferire qualcuno.

La **ludopatia**, poi, ha ottenuto dalla rete non solo una serie capillare di "centri" in cui spendere la propria "scommessa" (dalle edicole, ai bar, alle sale gioco), ma

viene ormai servita a domicilio e addirittura promossa attraverso pubblicità che ci giungono dai nostri televisori domestici, con l'ipocrita raccomandazione di essere moderati nell'esercizio di tali pratiche.

Nell'uno e nell'altro caso le cronache ci hanno descritto anche episodi estremi di suicidio, particolarmente toccanti quando si è trattato di giovani o giovanissimi. Gli operatori del volontariato hanno richiamato l'attenzione sulle "**nuove povertà**" che si legano a questi comportamenti, per cui possiamo oggi dire che il disagio psicologico non è meno frequente del disagio economico da parte di certe categorie e di un numero di individui sempre crescente.

Questa situazione richiede un impegno sempre più consapevole e professionale anche delle forze di polizia, alla ricerca di un equilibrio difficile da conseguire tra repressione, prevenzione e collaborazione con tutte le istituzioni e le attività sociali che cercano di gestire questo profondo cambiamento ottimizzando le opportunità (che sono molte) e contenendo i rischi (che sono gravi e facilmente riproducibili attraverso i meccanismi dell'emulazione e dell'imitazione).

Gli esempi si potrebbero moltiplicare, rendendo evidente non solo l'esigenza repressiva ma ancor prima, importantissima, come si diceva, l'esigenza informativa e preventiva da parte degli organi di polizia, in collaborazione con gli altri operatori sociali, come educatori, psicologi, medici, rappresentanti di genitori, ecc.

UNA PREPARAZIONE E UN AGGIORNAMENTO COSTANTI: UN DOVERE CIVICO E UNA SODDISFAZIONE PROFESSIONALE

Per muoversi efficacemente in questo **"mondo due virtuale"** occorre sempre più

avere una forte preparazione e un aggiornamento costante, che giustamente anche il sindacato si incarica di promuovere e incoraggiare in vari modi e in particolare con questo manuale. Bisogna subito aggiungere che questa attività di studio, di riflessione e di ricerca, se da una parte rappresenta un impegno, dall'altra costituisce anche una soddisfazione: quella di acquisire un ruolo sempre più consapevole ed attivo nella complessa trama di attività che il mantenimento dell'ordine pubblico comporta. In altre parole, un punto in avanti nella scala di dignità del proprio lavoro.

Questa preparazione e questo aggiornamento devono tenere conto di alcuni elementi fondamentali. Cerchiamo qui di indicarne i principali.

1. Il "mondo due virtuale" costituisce **un universo in continua espansione**. Anzi possiamo dire che siamo solo agli inizi di questa trasformazione che non è solo esterna a noi, ma investe anche la nostra mente, la nostra sensibilità, le nostre coscienze. Uno studioso di comunicazione ha infatti definito i media "protesi del nostro sistema nervoso centrale". Ciò significa che bisogna tener conto, anche nell'interpretazione delle leggi di tutela, che la persona è influenzata da tali strumenti fin nelle fibre più profonde della sua personalità, per cui l'azione repressiva non può mai essere disgiunta da un'azione di recupero e prima ancora di comprensione profonda delle dinamiche derivanti dall'esposizione a fenomeni che agiscono in profondità.
2. Questa considerazione matura dei meccanismi psico-fisici derivanti dal contatto con i media e ha come conseguenza il fatto che l'operatore che agisce con perizia e consapevolezza accresce notevolmente la **reputazione propria e del corpo cui appartiene**, in un equilibrio tra

attività di indirizzo e attività di contenimento delle deviazioni. Un corpo della pubblica amministrazione come quello della Polizia di Stato che sappia dimostrare sul campo un'adeguata professionalità in un settore avanzato come quello dell'informatica e dei processi digitali segna un significativo punto a favore che viene apprezzato non solo dalle autorità preposte ma dall'insieme dei cittadini, che richiedono un'impostazione moderna, al passo con i tempi e aperta agli sviluppi futuri.

3. Ed a proposito di tali sviluppi, bisogna essere consapevoli che siamo in presenza di un'evoluzione che, per quanto ci sorprenda e ci impegni, in realtà è appena cominciata. Basti pensare che il **Web invisibile** (conosciuto anche come **Web sommerso**), che è l'insieme delle risorse informative del World Wide Web non segnalate dai normali motori di ricerca, è già ora cento volte superiore al **Web conosciuto e praticato.** Infatti, secondo un'indagine sulle dimensioni della rete condotta da Bright Planet, un'organizzazione degli Stati Uniti d'America per le ricerche sulle caratteristiche del mondo digitale, il Web è costituito da oltre 550 miliardi di documenti mentre Google ne indicizza solo 2 miliardi, ossia meno dell'uno per cento.

4. Naturalmente gli operatori di polizia non debbono trasformarsi tutti in ingegneri informatici, né in programmatori di computer, ma debbono avere coscienza della sfida cui sono chiamati nel **controllo di questo enorme patrimonio virtuale**, diventando sempre più coscienti dei suoi sviluppi con le potenzialità positive che li accompagnano ma anche con i rischi. E come sappiamo chi persegue un intento fraudolento diventa particolarmente abile nel percorrere le strade del "sommerso" a preferenza di quelle dell' "esplicito".

IL CASO DI BITCOIN: VERSO UNA MONETA VIRTUALE

Si diceva che è questa una sfida che è solo agli inizi. Il nostro legislatore – com'è ampiamente documentato in questo manuale – ha già attrezzato gli organi di polizia e la magistratura di regole e strumenti efficaci. Ma la realtà tende ad evolversi più velocemente delle leggi. Negli scenari economici, ad esempio, si sta affermando ormai la presenza in rete dei **Bitcoin**, della moneta virtuale. "Mai più contante: rivoluzione in arrivo", titolava recentemente una rivista in materia. Ed aggiungeva: "Un mondo in cui ogni transazione avverrà senza contanti sarà più efficiente, con vantaggi e risparmi per i consumatori e mercati più trasparenti. Ma la strada della sicurezza è ancora lunga, soprattutto in Italia".

Questa evoluzione non deve stupire, dal momento che già ora non solo i grandi patrimoni, ma anche i risparmi dei comuni cittadini depositati negli istituti di credito sono espressi attraverso rappresentazioni virtuali, che vanno dai rendiconti numerici ai bancomat, dalle carte di credito ai riepiloghi delle cartelle-titoli.

Ma il Bitcoin è un ulteriore salto in avanti. Perché i depositi presuppongono, come dice il termine stesso un "deposito" di ricchezza tradizionale (un immobile a garanzia, la consegna di carta-moneta, ecc.), mentre la moneta elettronica ha una vita a sé. Riprendendo la nostra immagine, esso è un nuovo elemento del "mondo due" che non ha corrispondenza con un elemento del "mondo uno". Un grande salto concettuale e pratico, con interessanti aspetti positivi, ma anche con rischi di lesione dei diritti concreti della persona che accetta di operare in un settore tanto innovativo.

Nel giro di soli 5 anni (Bitcoin è stata creata nel 2009), questa moneta virtuale ha

ottenuto uno sviluppo che esige oggi di essere attentamente disciplinato. A differenza della maggior parte delle valute tradizionali, Bitcoin non fa uso di un ente centrale: esso utilizza un database distribuito tra i nodi della rete che tengono traccia delle transazioni, e sfrutta la crittografia per gestire gli aspetti funzionali come la generazione di nuova moneta e l'attribuzione di proprietà dei bitcoin, cioè di unità monetarie virtuali.

La rete Bitcoin consente il possesso ed il trasferimento anonimo delle monete; i dati necessari ad utilizzare i propri bitcoin possono essere salvati su uno o più personal computer sotto forma di "portafoglio" digitale, o mantenuti presso terze parti che svolgono funzioni simili ad una banca. In ogni caso, i bitcoin possono essere trasferiti attraverso Internet verso chiunque disponga di un "indirizzo Bitcoin". La struttura peer-to-peer della rete Bitcoin e la mancanza di un ente centrale rende impossibile per qualunque autorità, governativa o meno, di bloccare la rete, sequestrare bitcoin ai legittimi possessori o di svalutarla creando nuova moneta. Siamo insomma in presenza di una rivoluzione finanziaria virtuale che le istituzioni e gli organi responsabili non possono ignorare.

UNA STRATEGIA GLOBALE PER AFFRONTATE IL WEB

Di fronte a un cambiamento così profondo e complesso, occorre una strategia globale che sia composta sia di leggi efficaci, come quelle descritte in questo manuale, sia di prassi efficaci a monitorare il fenomeno. Bisogna infatti acquisire la capacità di governare il cambiamento facendosi trovare pronti di fronte alla sua evoluzione e non intervenendo in emergenza quando ormai i giochi sono fatti. Torna alla mente l'antico proverbio: non chiudere le porte della stalla quando ormai i buoi sono scappati, ma al contrario saperli accudire nella loro crescita.

In un contesto dove questa nuova realtà virtuale influisce sempre più profondamente nella quotidianità di ognuno di noi, è oggi indispensabile potenziare l'attività su questa tematica, utilizzando al meglio le elevatissime professionalità presenti nella specialità della Polizia Postale.

Tenendo conto delle ricerche in materia di sviluppo del Web e del suo impatto sociale, si possono individuare le seguenti azioni, che sono state indicate dall'Associazione e-Tutor Web nata recentemente per favorire l'alfabetizzazione informatica a tutti i livelli, dalle scuole al mondo del lavoro, dai giovani fino agli anziani:

- **Fornire gli strumenti** per un uso consapevole dei media e del web, informando gli utenti delle conseguenze negative , sul piano psicologico, relazionale e legale di un utilizzo non consapevole.
- **Individuare** le dinamiche, il funzionamento e l'approccio ai social network, l'intreccio tra reale e virtuale, gli interessi economici in gioco, i pericoli della messaggeria istantanea.
- **Guidare alla cultura della comunicazione** mediata dal computer attraverso il giusto rapporto tra la tecnologia e la quantità di dati che si possono produrre, raccogliere, scambiare e condividere.
- **Educare al dialogo attraverso i social-network** perché la comunicazione virtuale è ben diversa dalle interazioni della vita quotidiana, dove ci sperimentiamo nel contatto "faccia a faccia" con gli altri e mettiamo in gioco le nostre capacità relazionali.
- **Prevenire ludopatie, cyber bullismo, cybercrime, pedopornografia,** vere malattie del nostro tempo. E' indispensabile avviare un'informazione corretta e educare le persone sul rapporto da instaurare con il denaro e il

gioco. Mettere in guardia sul pericolo del "flaming", sul furto d'identità, insegnare a proteggere la privacy, individuare, prevenire e sanzionare le transazioni fraudolente.

- **Indicare le buone pratiche per il web 2.0** e colmare il divario tra i "social born", detti anche "nativi digitale" e gli "importati digitali", cioè i soggetti più anziani che hanno dovuto imparare il linguaggio del Web in età più matura.
- In questo senso gli organi responsabili della pubblica sicurezza devono **conoscere e coordinarsi con tutte quelle forme istituzionali e associative**, operanti soprattutto nel settore formativo e del volontariato che possono aiutare a partire dai social media usati con competenza, per promuovere e diffondere piattaforme per l'approfondimento e il dibattito, realizzare iniziative in grado di generare reti e alleanze tra agenzie educative, per orientare le scelte dei cittadini e farli diventare, finalmente, i veri protagonisti della comunicazione.
- **Diffondere la netiquette** che è l'insieme delle regole che dettano i parametri di educazione e buon comportamento in rete.
- **Favorire le tecniche divulgative** che sappiano indirizzare il pensiero e le azioni ad un uso consapevole degli strumenti informatici.
- **Affiancare, anche mediante le opportune collaborazioni, un'assistenza psicologica** che sia in grado di contrastare l'uso patologico della rete. L'eccessiva fruizione di internet è contraria alla socialità intesa come relazione perché favorisce l'isolamento, con il rischio di giungere ad una forma di autismo digitale dove alle persone si sostituisce la loro immagine virtuale.

- **Prevedere i necessari interventi giuridici e giudiziari** per stabilire la giusta relazione tra diritto e informatica ed evidenziare i rischi cui si può essere esposti da un cattivo uso degli strumenti digitali.

INTRODUZIONE

L'obiettivo della presente pubblicazione ha lo scopo di illustrare sommariamente gli aspetti più importanti di fenomeni criminali che hanno assunto col tempo una dimensione trasnazionale.

Sono i crimini ed i reati Informatici che si caratterizzano nell'abuso della tecnologia informatica sia hardware che software e che pongono a rischio i sistemi informativi di sicurezza nazionale.

Infatti l'evoluzione della tecnologia informatica e telematica e l'utilizzazione sempre più intensa ed estesa di impianti di elaborazione e trasmissione elettronica dei dati ha originato fenomeni quali l'e-commerce, l'e-government, l'home banking, il trading on-line e altre attività che rappresentano il mutamento della società e dei rapporti sociali.

Si ponga attenzione al fatto che oggi la maggior parte delle attività lavorative e di svago passano attraverso la rete informatica e i sistemi telematici.

Sicché si è reso necessario un intervento del legislatore, il quale ha introdotto nell'ordinamento giuridico una specifica legislazione penale, la legge 23 dicembre 1993 n. 547, finalizzata a regolare comportamenti socialmente dannosi o pericolosi, legati alle nuove tecnologie e per tutelare il diritto dell'individuo dalla indebita utilizzazione delle tecnologie informatiche e telematiche e, di conseguenza, dalla illegittima interferenza nella sfera privata, mediante l'utilizzo dei suddetti strumenti informatici.

Nel nostro ordinamento giuridico, prima dell'introduzione della suddetta legge n. 547/93, la materia dei reati informatici è stata oggetto di sporadici interventi settoriali, tra i quali si annovera la legge 1° aprile 1981 n. 121, contenente il

“Nuovo ordinamento dell’Amministrazione della Pubblica Sicurezza”, istitutiva di un Centro di elaborazione dati presso il Ministero dell’Interno e rappresentativa della prima forma di tutela di dati archiviati in un sistema informatico.

In definitiva, con la legge 547/93 il legislatore ha introdotto nuove norme nel sistema penale (i c.d. reati informatici) in riferimento alle attività criminose lesive di interessi di particolare rilievo nel settore informatico (cybercrime), quali: truffe, frodi mediante clonazione di carte di pagamento, accesso all’home banking, furti di dati per violazione dei diritti d’autore e utilizzo illecito del copyright, traffico d’armi, pedopornografia, stalking, telefonia, e-commerce, terrorismo, atti eversivi, stupefacenti, prostituzione, attentato ad impianti di pubblica utilità, violenza sui beni informatici, etc..

In questa prospettiva se i dati trasmessi attraverso i canali telematici fossero oggetto di strumentalizzazione da parte dell’operatore, quest’ultimo commetterebbe consapevolmente un illecito.

Il manuale dopo aver tracciato brevemente alcuni cenni storici sul crimine informatico ed aver preso in considerazione le disposizioni di cui si compone la normativa, passerà all’analisi dei singoli casi specifici in cui si riscontrano reati informatici, ovvero i settori di intervento della legge 547/93.

La Polizia di Stato, nell’ambito dei reati commessi attraverso l’utilizzo di strumenti informatici e telematici, svolge una costante attività di polizia giudiziaria diretta a monitorare la rete internet, per contrastare comportamenti socialmente dannosi o pericolosi posti in essere con l’ausilio di detti strumenti che mirano a danneggiare i suddetti sistemi.

In particolare la Polizia Postale e delle Comunicazioni ha la competenza specifica in materia di criminalità informatica e telematica.

La Polizia Postale e delle Comunicazioni è infatti una delle specialità di punta della Polizia di Stato, che oltre alla Polizia di Frontiera, alla Polizia Stradale, alla Polizia Ferroviaria etc., costituisce un Organo Centrale di intelligence del Ministero dell'Interno, Dipartimento della Pubblica Sicurezza – Direzione Centrale delle Specialità, e svolge funzioni inerenti la sicurezza e la regolarità nei servizi delle comunicazioni.

In sintesi, la Polizia Postale e delle Comunicazioni è il Reparto specializzato che ha il compito di prevenire e reprimere i reati e gli illeciti penali e amministrativi che rientrano nella vasta e complessa materia delle comunicazioni, incluse le attività illecite perpetrate per mezzo delle reti internet.

In conclusione, questo libro può essere un buon punto di partenza per la conoscenza dei problemi legati alla tutela del diritto dell'individuo dalla indebita utilizzazione delle tecnologie informatiche e di conseguenza dalle illegittime interferenze nella sfera privata, attraverso l'uso degli strumenti informatici e telematici.

Cari colleghi e lettori, auspichiamo che questo volume possa esservi di aiuto nella vostra vita quotidiana e nella vostra attività professionale, per meglio inquadrare i rischi dei reati informatici e valutare l'importanza che rivestono gli strumenti di tutela a salvaguardia della sicurezza della collettività. Detto ciò, ci è gradito segnalarvi che questo testo è il frutto delle esperienze professionali maturate sul campo da alcuni nostri validi amici e colleghi, nello specifico: Pasquale ALESSI, Vincenzo D'AGOSTINO, Antonio DEIDDA, Walter DELL'ARCIPRETE, Davide PARTITI e

Michele STRAGAPEDE, i quali con il loro prezioso e qualificato contribuito hanno consentito la realizzazione di questo interessante lavoro, avendo gli stessi svolto gran parte della loro attività professionale ed operativa occupandosi in prima persona di reati informatici e telematici e di strumenti di tutela. A loro, anche da parte nostra, va un sentito ringraziamento per il prezioso contributo fornito per la realizzazione di questo particolare ed utile strumento che auspichiamo possa accompagnare nel loro lavoro tutti gli operatori della Polizia di Stato e tutti coloro che lo utilizzeranno.

Un particolare ringraziamento va senza dubbio tributato al chiarissimo Professore Gianpiero Gamaleri, uno dei massimi esponenti del mondo della comunicazione, che ha curato la prefazione del volume, fornendo un autorevole e straordinario contributo per la realizzazione di questo prezioso testo che sicuramente darà significative risposte e spunti propositivi nel prossimo futuro, al fine di trovare soluzioni adeguate alle attuali problematiche per combattere efficacemente i rischi dei reati informatici e telematici ed individuare nuovi strumenti di tutela.

*Felice Romano **

*Michele Alessi ***

**Segretario Generale Nazionale Siulp*

***Presidente Associazione "Sicurezza, Giustizia, Legalità – Osservatorio per l'Europa"*

1) CENNI STORICI

La prima disposizione di legge organica in Italia in materia di contrasto al *cybercrime* è costituita dalla legge 23 dicembre 1993, n. 547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"), che costituisce un'adeguata tutela giuridica di fronte alla crescente diffusione di illeciti legati alla nuove tecnologie con rilievo nel settore informatico, e trae impulso da una disposizione comunitaria (la raccomandazione "*sur la criminalité en relation avec l'ordinateur"*adottata dal Comitato dei Ministri del Consiglio d'Europa il 13 settembre 1989).

La necessità di un intervento volto a regolare comportamenti socialmente dannosi o pericolosi ai settori dell'informatica e telematica era stata infatti avvertita fin dai primi anni ottanta sì da indurre numerosi Stati, sia europei che extraeuropei, a dotarsi di una specifica legislazione penale.

Ci si rese conto, in definitiva, che le forme di delinquenza tradizionale, con la diffusione delle tecnologie informatiche, erano state alterate e quindi "innovate" con nuove fattispecie criminose, che possono essere realizzate solo nell'ambito dei nuovi sistemi di comunicazione digitale.

In altre parole, il nascente bisogno di tutela di impianti di elaborazione e trasmissione elettronica dei dati informatici risponde ad una esigenza primaria di tutela dell'individuo nei confronti di indebite utilizzazioni delle tecnologie stesse, con interferenza nella vita privata.

Così nel 1996 fu istituito un Comitato Europeo per i Problemi Criminali (C.E.P.C.) composto da esperti per elaborare una convenzione internazionale per contrastare il crescente fenomeno *cybercrime.*

Detto organismo europeo elaborò un progetto che fu analizzato dal Consiglio d'Europa e aperto alla firma il 23 novembre 2001 in occasione della conferenza sul *cyber crime* tenutasi a Budapest.

La suddetta Convenzione di Budapest è stata ratificata nel nostro ordinamento con la legge 18 marzo 2008, n.48, promulgata dal Presidente della Repubblica e pubblicata in Gazzetta Ufficiale il 4 aprile 2008, n. 80, che rubrica "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di attuazione".

Oltre alle citate leggi del 23 dicembre 1993, n. 547 e del 18 marzo 2008, nr. 48, costituiscono l'infrastruttura su cui poggia il diritto penale dell'informatica, sia la legge 3 agosto 1998, n. 269 ("Norme contro lo sfruttamento della prostituzione, della pornografica del turismo sessuale in danno di minori, quali nuova forma di riduzione in schiavitù), sia il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

Meritano, altresì, menzione altri importantissimi interventi legislativi, quali:

- La legge 22 aprile 1941, n. 633 ("Protezione del diritto d'autore e altri diritti connessi al suo esercizio");
- Decreto Legislativo 21 febbraio 2014, n. 22 "Attuazione della direttiva 2011/77/UE che modifica la direttiva 2006/116/CE concernente la durata di protezione del diritto d'autore e di alcuni diritti connessi";
- Decreto legislativo 9 aprile 2003, n. 70, recante "Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno"

- "Delibera n. 680/13/CONS del 12 dicembre 2013", dell'Autorità per le Garanzie nelle Comunicazioni (istituita con la legge 31 luglio 1997, n. 249) inerente il Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70. Questa delibera è in vigore dal 31 marzo 2014.
- la legge 21 maggio 2004, n. 128 ("Conversione in legge, con modificazioni, del decreto legge 22 marzo 2004, n. 72, contenente interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo");
- Decreto legislativo 1° agosto 2003, n. 259 ("Codice delle comunicazioni elettroniche").
- Decreto legislativo 31 luglio 2005, n. 177 ("Testo unico dei servizi di media audiovisivi e radiofonici").
- Decreto legislativo 6 settembre 2005 , n.206 ("Codice del consumo").
- Codice Civile Artt. dal 1469-bis al 1469-sexies relativi alle clausole vessatorie nel contratto tra professionista e consumatore.

2) LA LEGGE 23 DICEMBRE 1993 N. 547

La legge n. 547/1993 ha introdotto nella legislazione italiana 14 nuove norme penali, idonee a sanzionare determinati fatti illeciti in ambito informatico o telematico, e distribuite interamente nel libro II di cui nove nel Titolo XII (Delitti contro la persona), Capo III (Delitti contro la libertà individuale), Sezione IV (Delitti contro la inviolabilità del domicilio), due nel Titolo XIII (Delitti contro il patrimonio), una nel Titolo III (Delitti contro l'Amministrazione della Giustizia), Capo III (Tutela

arbitraria delle private ragioni), una nel Titolo V (Delitti contro l'ordine pubblico), una nel Titolo VII (Delitti contro la fede pubblica), Capo III (Falsità in atti).

La legge n. 547 del 1993 interviene principalmente in quattro direzioni:

a) Le "frodi informatiche", che si caratterizzano rispetto alla truffa per il fatto di essere perpetrate servendosi dello strumento informatico e quindi senza induzione in errore di alcuno;
b) Le condotte di "falsificazione" estese ai documenti pubblici e privati, predisposti da un sistema informatico e telematico che, in quanto tali, non rientrano nel concetto tradizionale di documento;
c) Le "aggressioni alle integrità dei dati e dei sistemi informatici" previste mediante integrazione delle fattispecie tradizionali;
d) Le "aggressioni alla riservatezza dei dati e delle Comunicazioni informatiche", represse alla stregua delle altre forme di intrusione nella sfera privata.

L'accesso abusivo è chiaramente classificabile quale reato comune, infatti può essere commesso tecnicamente da chiunque.

Quindi il soggetto attivo, c.d. *hacker,* verosimilmente, deve perlomeno possedere delle conoscenze tecniche minime che gli consentano di porre in essere il proprio intendimento, ovvero deve possedere la capacità di commettere il fatto - reato.

Mentre il soggetto passivo è la persona fisica o giuridica, titolare del sistema informatico o telematico e al quale spetta il relativo *ius excludendi alios.*

Le condotte punite dalla norma sono:

1) l'introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza;

2) il mantenersi nel medesimo contro la volontà espressa o tacita di chi ha il diritto di escluderli.

L'oggetto materiale del reato è il sistema informatico o telematico.

Mentre il bene giuridico tutelato, che costituisce l'oggetto giuridico, è il c.d. "*domicilio informatico"* da intendersi come spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, il quale deve essere salvaguardato al fine di impedire non solo la violazione della riservatezza della vita privata, ma qualsiasi tipo di intrusione anche se relativa ai profili economico-patrimoniali dei dati.

Per la configurazione del reato informatico è richiesto il dolo generico, vale a dire la coscienza e volontà di porre in essere la condotta tipica che consiste nella volontà di introdursi o di mantenersi nella memoria interna di un elaboratore, in assenza del consenso del titolare dello *ius excludendi,* e con la consapevolezza che quest'ultimo ha predisposto delle misure di protezione per i dati che vi sono memorizzati.

L'art. 47, c.p., nel primo comma, disciplina l'ipotesi che esclude la punibilità nel caso di errore incidente sul processo di formazione della volontà, e prevede che "*l'errore sul fatto che costituisce il reato esclude la punibilità dell'agente*".

Ne consegue che la norma esclude la punibilità dell'agente, che per errore, si sia rappresentata una situazione che lo legittima ad accedere, con particolari modalità, nel sistema o a permanervi.

3) FATTISPECIE DI REATO

In ordine alle modalità dell'intervento apprestate dalla legge n. 547/1993 si denota: da un lato, la previsione di nuove figure criminose disciplinate da norme *ad hoc* e collocate nel tessuto normativo esistente.

Si pensi all'art. 615 ter c.p., relativo all'accesso abusivo ad un sistema informatico o telematico; all'art. 635 bis c.p. che disciplina il danneggiamento di sistemi informatici o telematici; all'art. 640 ter c.p. che rubrica frode informatica.

Dall'altro lato la dilatazione di fattispecie già contemplate con disposizioni che dettano definizioni ed introducono concetti.

Si pensi, in via esemplificativa ma non esaustiva: all'art. 392 c.p., che disciplina l'esercizio arbitrario delle proprie ragioni con violenza sulle cose, dopo il secondo comma è inserito il terzo comma ex art. 1 legge 23/12/1993, n.547, che detta:" *si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico*";

all'art. 5 ex l. 547/93 c.p., che ha sostituito il quarto comma dell'art. 616 c.p., violazione, sottrazione e soppressione di corrispondenza, con il seguente: "*agli effetti delle disposizioni di questa sezione per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza"*;

all'art. 7 ex legge 547/93, nell'art. 621c.p., che rubrica rivelazioni del contenuto di documenti segreti, dopo il primo comma inserisce il seguente: "*agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni e programmi";*

all'art. 13 ex legge 547/1993, che al comma 1 dell'art. 25-*ter* del decreto-legge 8 giugno 1992, n. 306, convertito, con modificazioni, dalla legge 7 agosto 1992, n. 356, dopo le parole "*e di altre forme di telecomunicazione*", aggiunge le seguenti: "*ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici*".

a) IL REATO DI FRODE INFORMATICA

Passando alla disamina dei settori nei quali è intervenuta la legge n.547 del 1993, notiamo che uno dei più importanti è quello delle frodi informatiche, realizzate servendosi dello strumento informatico e quindi senza ricorrere alla induzione in errore della persona.

L'art. 10 *ex legge* 547/93 prevede una nuova figura di reato, la frode informatica, inserita nel codice penale all'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 sui 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.*

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'art. 640 c.p., ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante".

Ne discende dalla norma di cui all'art. 640 ter c.p., posta a tutela sia della riservatezza e della regolarità dei sistemi informatici sia del patrimonio altrui, che l'evento consiste nel conseguimento da parte del soggetto attivo di un ingiusto profitto con altrui danno.

La condotta posta in essere dal soggetto attivo, infatti, consiste nell'alterazione del funzionamento del sistema informatico o telematico ovvero in un intervento

non autorizzato sui dati, informazioni e programmi ivi contenuti.

Ne deriva, dunque, che il reato di truffa informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto, con relativo danno altrui.

Un Esempio è dato dal: "soggetto che sottrae 30.000 euro da un conto corrente, accedendovi tramite internet e operando immediati bonifici in favore del proprio conto corrente".

Non configura, invece, il reato di frode informatica l'indebito utilizzo di carte di pagamento magnetiche; per tale ipotesi delittuosa, che costituisce una particolare forma di frode informatica, è stata predisposta dal legislatore una disciplina *ad hoc*, inserita nell'art. 12 della legge n. 197/1991(normativa relativa all' antiriciclaggio del denaro).

b) IL REATO DI ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO

Per sistema informatico deve intendersi quel complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche.

L'art 4 ex legge 547/1993, per tutelare la riservatezza dei dati e dei programmi contenuti in un computer, ha introdotto nel codice penale l'art. 615 *ter* che disciplina l'ipotesi di reato di accesso abusivo a un sistema informatico o telematico.

L'art. 615 *ter* c.p., nello specifico, recita: *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da uno a cinque anni:

1) se 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;

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

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

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

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

Integra, dunque, il reato di accesso abusivo a un sistema informatico o telematico (art. 615 *ter c.p.)* la condotta del soggetto che, pur avendo titolo ad accedere al sistema, vi si introduca con la *password* di servizio per raccogliere dati protetti per finalità estranee alle ragioni di impiego o d'istituto e alle finalità sottostanti alla protezione dell'archivio informatico.

La norma incriminatrice non punisce soltanto l'accesso totalmente abusivo al

sistema informatico ma anche la condotta di chi vi si mantenga contro la volontà espressa o tacita di chi ha diritto ad escluderlo (*ius excludendi alios*).

Un esempio è dato dal: " *soggetto che copia dei file presenti nella memoria del computer dell'ente di appartenenza ove presta lavoro effettuato per scopi estranei alle ragioni di lavoro*".

Il reato si consuma, nel momento in cui il soggetto si introduce in un sistema informatico protetto rimuovendo o forzando i presidi di sicurezza posti a tutela del sistema stesso, od anche permanendo oltre il tempo ed al di fuori delle motivazioni per cui ha l'autorizzazione ad introdursi ed a permanere nel sistema informatico.

L'abusività della condotta del soggetto, inoltre, va verificata avendo riguardo al momento dell'accesso e non all'eventuale uso successivo dei dati.

c) IL REATO DI DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI

Altra nuova figura criminosa introdotta nel codice penale (Libro II, Titolo XII, Sezione IV- dei delitti contro la inviolabilità del domicilio), dall'art. 4 della legge 547/199 è quella contemplata nell'art. 615-*quater* c.p., ovvero la detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, che prevede: "*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 a 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 a un anno e con la multa sino a 5.164 euro.*

La pena è della reclusione da uno a due anni e della multa da 5.164 euro a10.329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617-quater".

Integra, pertanto, la fattispecie di reato di cui all'art. 615 *quater* c.p. la condotta di colui che si procuri abusivamente il numero seriale di un apparecchio telefonico cellulare appartenente ad altro soggetto, poiché attraverso la corrispondente modifica del codice di un ulteriore apparecchio (cosiddetta clonazione) è possibile realizzare una illecita connessione alla rete di telefonia mobile, che costituisce un sistema telematico protetto, anche con riferimento alle banche concernenti i dati esteriori delle comunicazioni, gestite mediante tecnologie informatiche.

Si cita l'esempio del: "*soggetto che consapevolmente acquista a fini di profitto un telefono cellulare predisposto per l'accesso alla rete di telefonia mediante i codici di altro utente (c.d. "clonato") si rende responsabile del delitto di ricettazione, di cui costituisce reato presupposto quello ex art. 615 quater c.p."*

d) IL REATO DI DIFFUSIONE DI PROGRAMMI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO

L'art. 4 della legge 547/1993 introduce nel codice penale anche il reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, contemplato dall'art. 615 *quinques* c.p., che dispone: *"Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a euro 10.329*".

Rientra, quindi, nella previsione del reato di cui all'art. 615 *quinques* c.p. la diffusione di un programma avente per scopo ed effetto l'alterazione di alcune funzionalità telematiche dei sistemi informatici

Ricorre invece il reato di danneggiamento od interruzione di un sistema informatico nel caso in cui l'agente, per insinuarsi forzosamente in un sistema informatico, al fine di reimpostare la connessione telematica utilizzata, ricorra all'uso dei c.d. "*dialer*" illegali (letteralmente "compositori"), programmi, appunto, in grado di alterare il sistema informatico contenente dati da altri predisposti,per connettersi a numeri a tariffazione speciale, ad insaputa dell'utente.

e) IL REATO DI INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

L'art. 6 della legge 547/1993 inserisce nel codice penale l'art. 617 *quater* che dispone:*"Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.*

Salvo che il fatto costituisca più grave reato, la stesa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) In danno di un sistema informatico o telematico utilizzato dallo stato o da altro

ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) *Da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri e con violazione dei doveri inerenti alla funzione del servizio, ovvero con abuso della qualità di operatore del sistema;*

3) *Da chi esercita anche abusivamente la professione di un investigatore privato*".

Il reato di intercettazione, di impedimento o interruzioni illecite di comunicazioni informatiche o telematiche attiene alla condotta di chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Pertanto, integra gli estremi del reato di cui all'art. 617 quater c.p., l'utilizzo da parte del titolare di un esercizio commerciale, mediante l'impiego di terminale di cui è dotato (c.d. Pos), di carta di credito contraffatta, atteso che detto utilizzo genera un flusso di informazioni da parte del sistema computerizzato, diretto all'addebito della spesa sul conto del titolare della carta di credito ed al corrispondente accredito a favore dell'esercente commerciale.

Rischia, invece, la condanna per divulgazione di immagini intercettate, il soggetto che trasmette immagini televisive rubate ai canali RAI usati per le comunicazioni di servizio – anche se si tratta di riprese dal contenuto satirico.

Il delitto previsto dall'art. 617 quater c.p. non presuppone necessariamente che colui il quale divulga conversazioni intercettate sia il medesimo soggetto autore dell'intercettazione.

E' punita anche la condotta del soggetto che è venuto comunque a conoscenza anche in modo non fraudolento di una c.d. "conversazione chiusa", o "da punto a punto", essendo destinate a rimanere riservate, e la diffonda tra il pubblico.

f) IL REATO DI INSTALLAZIONE DI APPARECCHIATURE ATTE A INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEFONICHE

L'art. 6 della legge 547/1993 introduce nel codice penale l'art. 617 *quinques* che disciplina il delitto di installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche, e che dispone: "*Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi è punito con la reclusione da uno a quattro anni.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617- quater".

La norma in esame garantisce alle comunicazioni informatiche la stessa tutela che il codice penale accorda alle comunicazioni epistolari, telegrafiche e telefoniche, fattispecie contemplate nel Libro II – Titolo XII – Sezione V (*dei delitti contro la inviolabilità dei segreti*), artt. 616 ss. c.p..

Il termine "intercettare le comunicazioni relative al sistema", utilizzato dalla norma *de qua*, vuol dire inserirsi nelle comunicazioni riservate traendone indebita conoscenza.

Mentre il termine "relative" utilizzato dalla norma in esame non implica che le comunicazioni tutelate siano esse stesse relative a un sistema telematico o informatico.

Si configura il reato di cui all'art. 617 *quinques* c.p., nel caso di installazione non consentita di apparecchiature di intercettazione di comunicazioni con un sistema telematico o informatico.

Sicché integra la fattispecie di reato di cui all'art. 617 – *quinques* c.p. l'abusiva

installazione di una apparecchiatura nel luogo in cui gli utenti comunicano con il sistema *Postamat*.

g) FALSIFICAZIONE, ALTERAZIONE, SOPPRESSIONE DI COMUNICAZIONI INFORMATICHE ACQUISITE MEDIANTE INTERCETTAZIONE

La legge 547/1993, con la previsione di cui all'art. 6, ha introdotto nel codice penale il reato rubricato dall'art. 617 *sexies* c.p. di falsificazione, alterazione o soppressione di comunicazioni informatiche acquisite mediante intercettazione.

L'art. 617 *sexies* c.p., aggiunto dall'art.6 della legge 547/1993, prevede: *"Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di una delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.*

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art.617 –quater c.p.".

Le ipotesi criminose contemplate dal primo comma dell'art. 617 – *sexies* c.p. sono distinte e autonome.

La condotta dell'agente deve avere ad oggetto una comunicazione di un sistema informatico o telematico destinata a rimanere riservata.

La previsione di cui all'art. 617 *sexies* c.p. richiede quale presupposto di reato la falsificazione o l'alterazione o la soppressione di una comunicazione relativa ad un sistema informatico o telematico.

h) DISTRUZIONE, DETERIORAMENTO, CANCELLAZIONE DI DATI, INFORMAZIONI O PROGRAMMI INFORMATICI

Nel codice penale è stato inserito dall'art. 9 legge 547/1993, sostituito dall'art. 5 legge 18 marzo 2008, nr. 48, l'art. 635 –*bis* c.p. che rubrica danneggiamento di informazioni, dati e programmi informatici, e che dispone: "*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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio".

La legge 457/1993, in tema di criminalità informatica, ha introdotto in materia una speciale ipotesi criminosa, la condotta consistente nella cancellazione di dati dalla memoria di un computer.

Occorre evidenziare, come affermato dalla Suprema Corte di Cassazione con una sentenza resa a Sezioni Unite, che tra il delitto previsto dall'art. 9 della legge 547/1993 – che ha introdotto l'art. 635 *bis* c.p. - sul danneggiamento di sistemi informatici e telematici e la fattispecie criminosa prevista dall'art. 635 c.p. – sul danneggiamento, esiste un rapporto di successione di leggi nel tempo, disciplinato dall'art. 2 c.p. (*Cass. Pen., Sez. Un., 09 ottobre 1996, n. 1282*).

i) DOCUMENTI INFORMATICI

L'art. 491-*bis,*introdotto nel codice penale dall'art. 3 della legge 547/1993, disciplina i "*Documenti Informatici*" e detta: "*Se alcune delle falsità previste dal presente capo riguardano un documento informatico pubblico o privato avente*

efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private". Per documento informatico si deve intendere qualunque supporto informatico contenente dati o informazioni o programmi specificamente destinati ad elaborarli.

La norma in esame di cui all'art. 491-*bis* c.p. sanziona la falsità sia concernente direttamente i dati o le informazioni dotati, già in sé, di rilevanza probatoria sia quella relativa a programmi specificamente destinati ad elaborarli.

Quindi si deduce che l'archivio informatico di una pubblica amministrazione non è altro che un registro, costituito da materiale non cartaceo, tenuto da un soggetto pubblico. Sicché il pubblico ufficiale che nell'esercizio delle sue funzioni, e facendo uso dei supporti tecnici di pertinenza della pubblica amministrazione, confezioni un falso atto informatico destinato a rimanere nella memoria dell'elaboratore, senza che sia stampato alcun documento cartaceo, integra con la sua condotta la fattispecie delittuosa di falsità in atto pubblico disciplinata dagli artt. 476 c.p. (falsità *materiale* commessa da pubblico ufficiale in atti pubblici), e 479 c.p. (falsità *ideologica* commessa da pubblico ufficiale in atti pubblici).

Altresì, integra il reato di cui agli artt. 476, co. 1 e 491 *bis* c.p., la condotta del pubblico ufficiale che, in qualità di addetto al servizio di inserimento dati nel sistema di verbalizzazione informatica, alteri documenti informatici pubblici relativi alla predisposizione di verbali di accertamento di violazione delle norme del codice della strada. Nel caso di specie non rileva la circostanza che il sistema informatico coesista con quello cartaceo di supporto (*Cass. Pen. 21 settembre 2005, n. 45313*).

I) ATTENTATI AD IMPIANTI DI PUBBLICA UTILITÀ

Per impianti si intendono il complesso di strutture, apparecchi, attrezzature,

congegni ed opere concorrenti ai fini dell'organizzazione e dell'esplicazione di una determinata attività. (Es.: centralina telefonica).

Invece, non rientra nella nozione di impianti la cabina telefonica la quale, consistendo in una apparecchiatura destinata all'uso pubblico del servizio telefonico, è soltanto uno degli elementi dell'impianto che concorrono nella realizzazione del medesimo servizio telefonico.

Il testo dell'art. 420 c.p., che originariamente constava di un secondo e terzo comma, è stato sostituito dall'art. 2 della legge 547/1993, e, attualmente, è del seguente tenore: "*Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni".*

Il legislatore, in definitiva, con la nuova formulazione dell'art. 420 c.p., (attentato ad impianti di pubblica utilità), sostituendo l'originario testo con quello di cui all'art.2 della legge 547/1993, ha inteso introdurre una nuova figura di reato diretta ad una più estesa tutela dell'ordine pubblico, sanzionando penalmente qualsiasi attività diretta a distruggere o danneggiare impianti di pubblica utilità o di ricerca o di elaborazione di dati, attività considerata per sé stessa idonea a turbare la serena e ordinata convivenza sociale, indipendentemente dal verificarsi, in concreto, del relativo turbamento.

Quindi, la norma incriminatrice, di cui all'art. 420 c.p., indipendentemente dall'idoneità dell'azione a produrre un concreto turbamento del senso di tranquillità e sicurezza della collettività, per assoluta presunzione di legge, mira a tutelare la lesione dell'ordine pubblico.

Sicché integra il reato di cui all'art. 420 c.p.(attentato a impianti di pubblica

utilità), colui che abbia posto in essere una condotta diretta a determinare un concreto turbamento dell'ordine pubblico, e non è richiesta che, per la consumazione del reato, si sia verificato l'effetto voluto dall'agente.

Si rende, infine, responsabile del delitto in esame, contemplato dall'art. 420 c.p., colui che, per le finalità indicate in detta norma, fa scoppiare bottiglie incendiarie (c.d. "bombe Molotov").

m) COMUNICAZIONI E CONVERSAZIONI

L'art. 8 della legge 547/1993 introduce l'art. 623-bis c.p. che disciplina le comunicazioni e le conversazioni telegrafiche, telefoniche, informatiche o telematiche.

L'art. 623-*bis* rubrica "*altre comunicazioni e conversazioni*", e detta: "*Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini od altri dati*".

L'introduzione della nuova figura di reato sanziona penalmente qualsiasi attività diretta a trasmettere immagini televisive rubate ai canali RAI usati per le comunicazioni di servizio.

Il soggetto che pone in essere tale condotta, contraria alla norma incriminatrice di cui all'art. 623-*bis* c.p., rischia la condanna per divulgazione di immagini intercettate, con conseguente risarcimento.

Sussiste il reato di cui al combinato disposto degli artt. 617-*bis* e 623-*bis* c.p., anche nel caso il soggetto attivo del reato installi un apparecchio ricevente atto ad intercettare le comunicazioni degli organi di polizia effettuate attraverso la

loro centrale operativa.

Infatti la norma di cui all'art. 623-*bis* c.p., come detto introdotta dall'art. 8 della legge 547/1993, si riferisce ad ogni genere di "*trasmissione a distanza di suoni, immagini ed altri dati*", e dunque senza il limite che dovesse trattarsi di trasmissione "*con collegamento su filo o ad onde guidate*".

n) SOSTITUZIONE DI PERSONA

Il Capo IV del Libro II del Titolo VII, disciplina "Delle falsità personali" e all'art.494 c.p., contempla il delitto di sostituzione di persona, posto a tutela dell'interesse riguardante la pubblica fede.

L'art. 494 c.p., che rubrica, come detto, "sostituzione di persona", recita: "*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno*".

Ne discende che integra il delitto di cui all'art. 494 c.p. la condotta di chi crea un indirizzo di posta elettronica spacciandosi per un'altra persona e intrattenendo rapporti con gli utenti della rete, con l'intento di arrecare danno al soggetto le cui generalità siano state abusivamente spese.
Nel caso di specie, si tratta di reato che lede l'interesse non solo riguardante la pubblica fede, ma anche quella privata e la tutela civilistica del diritto al nome, configurandosi una ipotesi che può superare la ristretta cerchia di un determinato destinatario.

Integra la fattispecie di reato in esame, anche, chi usando un falso contrassegno di identità, come il "nickname" avvia una corrispondenza su "*facebook*" con soggetti che altrimenti non gli avrebbero concesso la loro amicizia o corrispondenza.

In definitiva il fatto costitutivo del delitto di sostituzione di persona, di cui all'art. 494 c.p., consiste nell'indurre taluno in errore, sostituendo illegittimamente la propria, o all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità cui la legge attribuisce effetti giuridici.

Il delitto in esame si consuma nel momento in cui taluno è stato indotto in errore con i mezzi indicati dall'art. 494 c.p..

o) FURTO D'IDENTITÀ

La crescente evoluzione informatica e telematica, il massiccio uso di Internet, hanno determinato, come detto, il nascere di nuove ed importanti figure criminali, che hanno assunto, col tempo, dimensioni trasnazionali.

Inoltre, l'uso massiccio della posta elettronica, la diffusione delle transazioni telematiche, l'utilizzo dei social network e chat per condividere informazioni, hanno favorito e incrementato la circolazione di dati personali, rendendo così i navigatori vulnerabili alla possibilità di essere vittime di "furto d'identità".

Il "furto d'identità", ipotesi criminosa che ricade nella fattispecie di reato disciplinata dall'art. 494 c.p. (sostituzione di persona), **è** ogni condotta intrapresa al fine di ottenere, in modo fraudolento, un'informazione individuale, relativa sia a persone fisiche che aziende, con l'intento di utilizzare identità o dati personali altrui, per scopi illeciti.

Il "furto d'identità", ha per oggetto, dunque, l'identità di un'altra persona, mediante la quale il soggetto finge di essere qualcun altro, assumendo l'identità

di quella persona, di solito per accedere a risorse o ottenere crediti o altri benefici, spendendo il nome altrui.

Il "furto d'identità" può essere totale o parziale, secondo che l'appropriazione indebita d'identità altrui si consuma attraverso l'uso di nome di altre persone, realmente esistenti o decedute, o, quando, si utilizzano solo alcuni dati falsi, per conseguire un ingiusto profitto.

La Suprema Corte di Cassazione ha statuito che: " è configurabile il reato di sostituzione di persona nel caso in cui si apra un account di posta elettronica intestandolo a nome di altro soggetto, comportando ciò l'induzione in errore non tanto dell'ente fornitore del servizio quanto dei corrispondenti i quali si trovano ad interloquire con persona diversa da quella che ad essi viene fatta credere. (Cass. Pen. Sez. V 08/11/2007, n.46674).

Quindi bisogna prestare molta attenzione e non divulgare i dati propri personali in siti, tipo e-banking, in quanto l'acquisizione di identificatori personali è resa possibile grazie alla propria disattenzione che consente ai c.d. "ladri di identità" di appropriarsi dei propri dati personali e delle proprie credenziali di accesso.

4) MODIFICAZIONI ED INTEGRAZIONI DELLE NORME DEL CODICE DI PROCEDURA PENALE IN MATERIA DI CRIMINALITÀ INFORMATICA

La legge 547/1993 ha introdotto anche significative novità in ambito processuale, prevedendo negli artt. 11 e 12, alcuni aspetti propri della fenomenologia informatica.

Infatti l'art. 11 della citata legge 547/93 ha inserito nel Capo IV (intercettazioni di conversazioni o comunicazioni), del titolo III (mezzi di ricerca della prova), del libro III (prove), del codice di procedura penale, l'art. 266 bis, che rubrica

“Intercettazioni di comunicazioni informatiche o telematiche”.

La norma de quo è stata introdotta dal legislatore per consentire di annoverare “l’intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi”, tra i mezzi di ricerca della prova.

L’art. 12 della legge 547/93, invece, ha modificato l’art. 268 del codice di procedura penale, inserendo il comma 3 bis, e sostituendo i commi 6,7,8.

Il comma 3-bis dell’art.268 c.p.p, è stato introdotto dal legislatore nel caso in cui le Procure della Repubblica non fossero dotate di apparecchiature tecnologicamente all’avanguardia, ovvero, insufficienti ed inidonee, per svolgere intercettazioni di comunicazioni telematiche o informatiche.

In tal caso, il comma 3-bis, in esame, prevede che il Pubblico Ministero, con decreto adeguatamente motivato, può avvalersi, per lo svolgimento delle suddette operazioni di captazione, di impianti appartenenti a privati, ovvero di impianti in dotazione alla Polizia di Stato.

5) CYBER FORENSICS

L'informatica forense è la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione, l'impiego ed ogni altra forma di trattamento del "dato informatico" al fine di essere valutato in un processo giuridico.

Si tratta di una disciplina di recente formazione. Spesso viene erroneamente identificata come una nuova branca della computer security.

L'aspetto più noto e studiato dell'informatica forense è la "computer forensics" che si occupa, ai fini probatori, delle tecniche e degli strumenti per l'esame metodologico dei sistemi informatici, ma stanno acquisendo sempre maggiore

importanza anche altri aspetti legati all'impiego di tecnologie informatiche nell'ambito del processo.

Un tipico esempio è il cosidetto "esperimento giudiziale" virtuale in cui si impiega il computer per riprodurre un fatto attraverso la cd "realtà virtuale", tanto che si parla di "computer generated evidence".

Con l'aumento dei reati informatici e, soprattutto con una presa di coscienza da parte dei soggetti che hanno finalmente cominciato a denunciare i crimini di cui sono vittime, sarebbe opportuna un'applicazione sistematica integrale di questa disciplina, che sembra tuttavia non scevra di evoluzioni.

a) LA TUTELA DELL'INTEGRITÀ DEI DATI

Nell'ambito dell'informatica forense uno degli aspetti fondamentali è la salvaguardia dei dati presenti sui supporti di archiviazione posto sotto il vincolo del sequestro, dunque non nella disponibilità del proprietario. A salvaguardia dei dati e della garanzia di inalterabilità di questi ultimi, gli operatori della Polizia Postale preposti all'analisi dei dispositivi di archiviazione utilizzano determinate metodologie volte a garantire e provare l'esatta corrispondenza dei contenuti in qualsiasi momento dell'analisi. Per rendere possibile ciò occorre "congelare" il dato, ossia porre in essere tutti gli accorgimenti tecnologici atti ad impedire scritture (anche accidentali) di bit e a verificare che in un momento successivo i dati presenti siano gli stessi. Per adempiere a tali obblighi, oltre all'utilizzo di strumenti hardware o software che inibiscano qualsiasi scrittura sui dispositivi di archiviazione, vengono impiegati algoritmi di hash allo scopo di generare una sorta di impronta digitale di ciascun file e/o dell'intero contenuto del dispositivo, permettendo quindi di verificarne l'integrità in qualsiasi momento successivo al sequestro.

b) DIGITAL FORENSICS EXPERT

Il termine "computer forensics expert" è utilizzato per identificare la figura professionale che presta la sua opera nell'ambito dei reati informatici o del computer crime. Dal momento che non esiste una definizione univoca ricompresa nella dizione "informatica forense", esso deve occuparsi di preservare, identificare, studiare e analizzare i contenuti memorizzati all'interno di qualsiasi supporto informatico o dispositivo di memorizzazione. Qualsiasi dispositivo elettronico con potenzialità di memorizzazione dei dati (ad es. cellulari smartphone, sistemi di domotica, autoveicoli , navigatori gps, etc.)

c) FORENSICS ED INVESTIGAZIONI DIGITALE

La straordinaria e frenetica diffusione delle tecnologie digitali ha oramai influenzato in maniera decisiva ogni aspetto della vita e delle attività umane, determinando una rivoluzione nel modo di lavorare, di comunicare e divertirsi.

L'utilizzo intenso di tali tecnologie ha quindi causato l'aumento esponenziale dei dati e delle informazioni create, manipolate, memorizzate e trasmesse in formato digitale.

Si consideri infatti che ai giorni nostri il “patrimonio informativo” delle istituzioni, delle aziende e dei cittadini è pressoché totalmente digitalizzato e viaggia sulle reti telematiche. Così come le comunicazioni e le transazioni finanziarie.

Questo è il motivo per cui sempre con maggior frequenza i sistemi informatici e telematici sono “implicati” nella commissione di illeciti di vario genere e di conseguenza, contrariamente a quanto avviene in altri settori dell'indagine di polizia giudiziaria, è necessario continuamente aggiornarsi nelle procedure investigative.

Le investigazioni digitali devono quindi adeguarsi ai velocissimi cambiamenti delle predette tecnologie al fine di essere in grado di individuare e recuperare i dati digitali e le informazioni utili alle indagini e successivamente utilizzabili come prova valida davanti al giudice.

La Digital Forensics può essere definita come la disciplina che si occupa dello studio e dell'applicazione delle tecniche finalizzate ad individuare, acquisire, conservare, valutare analizzare e presentare i dati digitali in modo tale da essere validi a fini probatori.

Al suo interno vi è una serie enorme di specializzazioni tra le quali si citano, a titolo di esempio, la “computer forensics”, che si occupa prevalentemente dell'analisi delle memorie dei computer, la “mobile forensics” che tratta la sterminata categoria dei dispositivi “mobili” come i telefoni cellulari, gli smartphone ed i tablet, la “live forensics” che riguarda l'intervento su sistemi in funzione, la “image e video forensics” che riguarda le tecniche di analisi su immagini e video digitali.

Bisogna dire che i vari soggetti (P.G., A.G. avvocati, consulenti) che operano in questo settore incontrano serie difficoltà, dovute, non solo alla complessità ed alla dinamicità della materia, ma sopratutto all'attuale mancanza in Italia (ma anche all'estero) di una standardizzazione delle procedure e di un protocollo delle modalità operative. Benché in linea generale si potrebbe affermare che si dovrebbero utilizzare dei software dedicati con speciali dispositivi hardware o software che impediscano modifiche ai supporti originali durante il loro esame (write block). Allo scopo si segnala il sito “http://www.digital-forensics.it/acquisizione-con-ftk-imager”. Successivamente si dovrebbe effettuare sul posto una copia "forensic" degli hard disk o degli altri supporti di

memorizzazione, identica all'originale al fine di svolgere successivamente gli accertamenti. Ed infine, occorrerebbe calcolare l'hash dell'intero contenuto di ogni supporto acquisito (es. hard disk), allegando l'entità di tale valore al verbale redatto dalla P.G. al fine di assicurare la non disconoscibilità dei dati acquisiti. Allo scopo si segnala il sito "http://www.digital-forensics.it/hashing".

Le "prove digitali" hanno la caratteristica di essere immateriali e pertanto fragili e volatili; per questo sono facilmente soggette a subire alterazioni, dispersioni e danneggiamenti da parte di chi le manipola. Si intuisce quindi come sia estremamente facile e altamente probabile, anche senza volerlo, compromettere ed inquinare irrimediabilmente la scena del delitto, se non si possiede una adeguata preparazione e non si proceda con le necessarie cautele.

La perquisizione, il sequestro probatorio e l'ispezione sono gli strumenti tipici di ricerca ed acquisizione della prova e vengono utilizzati anche nel caso in cui si stiano trattando i reati oggetto di indagine informatica.

La promulgazione della legge 48/2008 ha fortunatamente sanato gli aspetti che rendevano incompatibile con l'immaterialità del dato informatico l'applicazione di taluni degli anzidetti strumenti.

Ad esempio nell'art. 247 del codice di procedura penale, che riguarda le perquisizioni, è stato inserito il comma 1 bis che testualmente recita:

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.

Anche l'art. 352 è stato significativamente modificato in modo da fornire

strumenti idonei a trattare i dati digitali con l'inserimento del comma 1 bis:

1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.

Anche l'art. 354 c.p.p., che riguarda gli accertamenti urgenti sui luoghi, sulle cose e sulle persone ed il sequestro, ha subito dopo la L. 48/2008 significative modifiche:

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.

2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la

conformità della copia all'originale e la sua immodificabilità. Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.

È utile sapere che nell'ambito dei reati informatici o di quelli commessi mediante le tecnologie informatiche, nei casi di pedopornografia online e di violazione delle norme relative al diritto d'autore è prevista la confisca come pena accessoria. In questi casi il sequestro deve obbligatoriamente riguardare anche gli strumenti utilizzati per la commissione del reato per cui gli organi di Polizia Giudiziaria che ne facciano richiesta possono ottenere detti beni sia in custodia con facoltà d'uso che assegnati definitivamente dopo l'eventuale confisca.

6) CENNI INFORMATICI

Fatta questa breve e sintetica illustrazione della legge 23 dicembre 1993, n. 547, di modificazione ed integrazione delle norme del codice penale e di procedura penale, in tema di criminalità informatica, che sanziona determinati fatti illeciti in ambito dei sistemi di comunicazione digitale, il manuale, nelle pagine che seguono, si arricchisce con i contributi offerti dagli operatori della Polizia di Stato, appartenenti alle varie specialità dalla Polizia di Stato,esplicatesi in suggerimenti, interpretazioni e materiale didattico, trasformando, in tal modo, in maniera sostanziale, la forma e il contenuto del compendio.

In ultima analisi si può ben affermare che il manuale sui "*sui rischi dei reati informatici*" è stato realizzato dalla Segreteria Generale del S.I.U.P., soprattutto con il prezioso contributo dei suddetti operatori, come detto esperti di differenti campi della Polizia di Stato, sospinti in questo dal comune spirito di *open source* (fonte comunicativa) che è alla base della "*galassia Internet*".

In special modo, nel loro contributo scritto i suddetti specialisti della Polizia di

Stato hanno posto l'accento sui rischi e le insidie, evidenziandoli, in cui possono incorrere coloro che, quotidianamente, utilizzano il sito Web.
Si rappresenta inoltre che gli stessi hanno suggerito possibili tutele da adottare per evitare indebite utilizzazioni della rete informatica o telematica da parte di soggetti, socialmente pericolosi, che possano con la loro condotta illecita, interferire nella vita privata degli individui/utenti che navigano in rete.
Sicché le pagine che seguono sono strutturate in una sequenza di argomenti che coprono alcune delle più importanti aree applicative di Internet.

6.1) PERSONAL COMPUTER – HARDWARE – SOFTWARE

Si comincia con il primo contributo offerto che è quello relativo alla macchina elettronica automatizzata, che è il personale computer, in grado di elaborare complessi calcoli matematici e di gestire enormi quantità di dati.

Il personal computer, è ampiamente utilizzato sia in ambito lavorativo/professionale, sia in ambito privato (c.d. "*domestico*"), e se ne fa frequente uso per la video-scrittura, per la contabilità, per l'elaborazione video, per le immagini e audio, per la progettazione in generale nei sistemi di sicurezza aziendali e privati.

Inoltre, la sua funzione, negli ultimi anni, con l'avvento e la diffusione di Internet, si è ulteriormente evoluta in modo tale da costituire un grande mezzo di libera comunicazione globale. Il personal computer nasce come una macchina elettronica automatizzata in grado di ricevere comandi, istruzioni o compiti dall'esterno (*input*), e, a seguito di elaborazione di calcoli matematici (algoritmi), ne favorisce un risultato e/o un esito, con l'invio di dati in uscita (*output*).

Per definizione il personal computer, dal punto di vista hardware è un sistema elettronico digitale (programmabile) che elabora cioè tutti i dati in formato

digitale o numerico, ovvero come sequenze 0 e 1 corrispondenti a due livelli di tensione (*alto e basso*), coincidenti a loro volta ai due stati fisici di interruttore aperto e chiuso, elaborando i dati in input e fornendo una soluzione output.

Il personal computer è formato da diversi componenti hardware, alcuni sono essenziali ed altri accessori; molti di tali componenti sono di utilizzo comune, molti altri sono, invece, riservati ad un uso professionale.

Un singolo componente hardware è definito anche "*device" o "periferica",* in relazione alla subordinazione all'unità centrale del componente stesso.

Il *"device",* in generale, tratta le informazioni input (ingresso) oppure di output (uscita); mentre vi sono dispositivi che possono elaborare informazioni sia di input che di output allo stesso tempo (ad es.: il masterizzatore DVD).

Il "*device*" è, dunque, uno strumento informatico che l'operatore utilizza quando ha necessità di eseguire appositi programmi software, detti di "*comando*", creati con lo scopo di interagire con il personal computer, utilizzando un linguaggio macchina o linguaggio hardware.

Il linguaggio macchina o linguaggio hardware è costituito da una sequenza di "*bit*", cui si associano per codifica altri linguaggi di più alto livello.

Si definisce "*bit*" la più piccola unità di memorizzazione di una informazione elementare, rappresentata da una cifra binaria che può assumere due soli stati: "*UNO*" e "*ZERO*".

Lo stato "*UNO*" indica "*ON*" (acceso), mentre lo stato "*ZERO*" indica "*OFF*" (spento).

I "*bit*", inoltre, vengono aggregati in gruppi di otto, denominati "*byte*" e, rappresentano caratteri, numeri o simboli.

In sintesi, l'unità di misura dell'informazione unitaria elementare è il "*bit*",

mentre il "*byte*" è un termine che sta ad indicare un insieme di otto "*bit*", e rappresenta un qualsiasi carattere.

Si riporta di seguito una tabella esplicativa contenente le unita di misura per la memorizzazione delle informazioni:

6.2) UNITÀ' DI MISURA PER LA MEMORIZZAZIONE DELLE INFORMAZIONI

Unità di misura	Simbolo	Capacità
Byte	**B**	**8 Bit**
Kilobyte	**KB**	**1024 byte**
Megabyte	**MB**	**1024 kilobyte**
Gigabyte	**GB**	**1024 megabyte**
Terabyte	**TB**	**1024 gigabyte**
Petabyte	**PB**	**1024 terabyte**
Exabyte	**EB**	**1024 petabyte**
Zettabyte	**ZB**	**1024 exabyte**
Yottabyte	**YB**	**1024 zettabyte**

Si sottolinea, alla luce della illustrata tabella esemplificativa dell'unità di misura per la memorizzazione delle informazioni, di prestare attenzione e di non confondere l'unità di misura "*Kilobyte*" (KB) con l'unità di misura "*Kilobit*". Quest'ultima unità di misura dell'informazione o della memoria dei vari multipli "*bit*", infatti, ha valore 1.000 "*bit*".

Il software, come già detto, è una componente del personal computer che consente l'utilizzo dei programmi, e si differisce dall'hardware perché quest'ultima componente è invece la parte fisica elettronica dell'elaboratore.

L'immissione dei dati in entrata (input) è di tipo alfa-numerico decimale per cui, per essere comprensibile all'elaboratore, è necessaria un'operazione di codificazione delle

informazioni in formato digitale o numerico con sequenze "0" e "1" (c.d. sistema binario), e, viceversa, occorre una codificazione inversa per una visualizzazione dei dati in uscita (output) da binario a alfa-numerico decimale.

In parole povere, ad ogni tipo di istruzione viene assegnato un codice binario, in quanto non sarebbe possibile utilizzare il formato binario per scrivere programmi. Pertanto, si utilizza una rappresentazione simbolica della codifica binaria. I codici usati per i dati alfanumerici sono:

1.EBCDIC (Extended Binary Code Decimal for Information Interchange);

2.ASCII (America Standard Code for Information Interchange).

L'elaborazione delle informazioni è affidata al processore o "*CPU"*(Central Processing Unit). Poiché il linguaggio macchina normalmente elaborato dalla "*CPU*", non è direttamente comprensibile, sono stati creati dei linguaggi appositamente studiati per rendere più semplici le operazioni di programmazione.

Va ricordato, inoltre, che l'utilizzatore medio impiega il computer attraverso l'interfaccia utente ("*UI*" – dall'inglese User Interface) che rappresenta la componente di un sistema software che consente l'interazione e la comunicazione dell'utente con il sistema informatico.

6.3) UN PERSONAL COMPUTER PUÒ ESSERE

a) <u>*PC desktop o fisso,*</u> è costituito da un "*case*"(involucro esterno di metallo o plastica che contiene i componenti principali del computer: scheda madre, scheda video, scheda audio, scheda di memoria, scheda della "*CPU*", hard disk, lettori cd-dvd, masterizzatore, lettore floppy disk, alimentatore..), un "*monitor*", una "*tastiera*", un "*mouse*" e altre periferiche esterne (modem, stampante, scanner…);

b) *PC portatile,* è un dispositivo di facile trasporto per l'utente, in cui sono integrate tutte le principali componentistiche hardware per il suo funzionamento;

c) *PC notebook,* è un PC portatile dalle dimensioni ancora più ridotte;

d) *PC tablet*, anch'esso è un PC portatile di ridotte dimensioni e, permette all'utente di interagirvi non a mezzo di una tastiera ma direttamente dallo schermo del PC tablet, sia con l'utilizzo di appositi pennini o direttamente con le dita (schermo tattile o touch-screen);

e) *PC palmare o PDA*, è sempre un PC portile dalle dimensioni tali da poter stare nel palmo di una mano, dotato di schermo tattile, inizialmente utilizzato come semplice agenda personale e calcolatrice, col tempo si è evoluto con funzioni più avanzate;

f) *Smartphone* è il telefono cellulare di ultima generazione, il quale svolge oltre il ruolo inziale di telefonia mobile, anche funzioni, simili se non superiori, di un palmare o quelle proprie di un PC portatile, ed è dotato o si possono installare numerose applicazioni in connettività.

7) I SISTEMI OPERATIVI

Il sistema operativo è un programma o software che consente il funzionamento del personal computer, permette all'utente di interagire con facilità con la macchina, che gestisce tutte le periferiche ivi installate, accorda, inoltre, la connessione alla rete Intenet.

I sistemi operativi a causa della loro complessità di progettazione possono essere oggetto di attacchi esterni, e possono avere dei difetti di programmazione. A tal proposito, in rete sono disponibili, periodicamente, le "*patch*" (pacchetti per la risoluzione di problemi ed implementazione della sicurezza), le quali, una volta

installate sul proprio personal computer sopperiscono alle varie problematiche che si presentano, di volta in volta.

I principali sistemi operativi sono il "*DOS*", il "*Windows*", il "*Mac Os*", l'"*Unix*", il "*Linux*"; mentre, per dispositivi mobili i sistemi operativi sono: ("*Android*", "*Mac Ios*", "*Symbian*", "*Windows Phone*"….).

8) INTERNET

Internet si può definire come una gigantesca "*ragnatela*" mondiale costituita da un'interconnessione di reti di computer che offre la possibilità agli utenti di accedere a svariati servizi ed informazioni.

Ma la definizione tecnica più corretta ed attuale di Internet è, forse, quella di una federazione o un insieme di reti in grado di comunicare utilizzando il set di protocolli "*TCP/IP*" (Trasmision Control Protocol / Internet Protocol).

Questo strumento di comunicazione, infatti, ha avuto un enorme ed inaspettata diffusione, ed invero si è prepotentemente imposto quale mezzo principale di interscambio di informazioni di qualsiasi natura.

Lo sviluppo della rete Internet ha origine da ARPANET, un network di computer messo in piedi nel settembre 1969, dalla Advanced Research Projects Agency (ARPA), per applicazioni militari.

ARPA, invece, è stata creata nel 1958 dal Dipartimento della Difesa degli Stati Uniti allo scopo di mobilitare risorse di ricerca, in particolare dal mondo universitario, verso la costruzione di una superiorità tecnologica militare sull'Unione Sovietica, subito dopo il lancio del primo Sputnik nel 1957.

In definitiva, lo scopo del Dipartimento della Difesa degli Stati Uniti era quello di stimolare, presso centri universitari, la ricerca sull'utilizzo interattivo del computer. Nel 1973 fu delineata da alcuni ricercatori nonché scienziati informatici, in un documento, l'architettura fondamentale di Internet.

Si comprese, allora, che le reti di computer per dialogare tra loro avevano bisogno di protocolli standardizzati,

E così il programma minore ARPANET fu trasferito alla Defense Communication Agency (CDA), al fine di rendere disponibile la comunicazione via computer a differenti settori delle forze armate. In sintesi, la CDA realizzò una connessione tra le reti sotto il suo controllo.

Ma il Dipartimento della Difesa preoccupato per possibili buchi nella sicurezza creò una rete MILNET, separata, per specifici impieghi militari.

Successivamente, nel 1984 la National Science Foundation (NSF) mise a punto una propria rete di comunicazioni via computer, utilizzando Arpa-Internet, come sua dorsale.

Nel 1990 ARPANET, oramai tecnologicamente obsoleta, fu smantellata.

In seguito Internet fu liberato dal suo ambiente militare e fu affidato alla National Science Foundation dal Governo degli Stati Uniti. Oramai la tecnologia informatica del networking era di dominio pubblico.

Ma ciò che ha permesso ad Internet di abbracciare l'intero mondo è stato lo sviluppo del software browser "*World Wide Web*", ovvero un'applicazione per la condivisione delle informazioni.

Ancora oggi Internet si fonda sull'architettura di comunicazione costruita su tre principi: a) una struttura di rete decentrate; b) una potenza di calcolo distribuito

attraverso tutti i nodi della rete; c)la sovrabbondanza di funzioni nel network per minimizzare il rischio di sconnessione. In Italia il software browser "World Wide Web" è stato rilasciato in rete dal CNR nell'agosto del 1991.

Ciò ha permesso il diffondersi della disponibilità generalizzata di accessi ad Internet, su rete telefonica analogica.

Alla luce di questi brevi cenni storici sulle origini di Internet, occorre evidenziare che il linguaggio comune che permette ai computer interconnessi (host) di comunicare fra loro è garantito dai protocolli di rete (i principali sono "*TPC/IP"*), indipendentemente dalla loro struttura hardware e software.

Al momento, Internet come diffusione mondiale è secondo solo alla rete telefonica generale, ma con l'implementazione e lo sviluppo della tecnologia "*Volp*", sicuramente prevarrà sulla stessa rete telefonica.

Inoltre, per accedere alla rete Internet e utilizzarne i suoi molteplici servizi, occorre essere forniti di un computer munito di modem o di un router e dei relativi programmi, se si utilizza una rete locale da connettere a Internet ed instaurare una connessione con "Internet Provider Service" (IPS) che rappresenta il fornitore dei servizi Internet, previa stipula contratto di servizio.

La stipula del suddetto contratto di servizio permette l'accesso ad Internet attraverso o una linea di telecomunicazioni specifica (quale wireless o cablata, satellitare mono o bi-direzionale Adsl Wi-Fi, Skylogic..) o a mezzo di una linea telefonica generica (Isdn, Gsm, Umts, Hdspa, Lte ovvero il cosiddetto 4 G..), consentendo così di "*navigare*" con un apposito programma chiamato "*Web Browser*".

8.1) GLI INDIRIZZI "IP"

Un indirizzo "IP" (*Internet Protocollo Address*) è una etichetta numerica che identifica, univocamente, un dispositivo (*host*) collegato a una rete informatica, che utilizza l'"Internet Protocol" come protocollo di comunicazione.

Quindi, un computer, una volta che viene connesso a una rete, è identificato attraverso "l'IP"; una sorta di numero di targa, che caratterizza lo stesso computer sulla rete informatica. Esso si presenta come una serie di 4 numeri di valore compreso tra 0 e 225, separati da un punto (*es.:192.168.1.1*).

L'indirizzo "IP", come detto, identifica un dispositivo sulla rete, e, ne traccia, di conseguenza, il relativo percorso per la sua raggiungibilità da un altro dispositivo in rete, in una comunicazione dati "a pacchetto".

Gli indirizzi "IP" possono essere pubblici o privati, dinamici e statici.

Sono indirizzi "IP" pubblici quelli rilasciati e disciplinati dall'ICANN (*Internet Corporation for Assigned Names Numbers*), Ente internazionale costituito nel 1993 su mandato del Dipartimento per il Commercio statunitense.

L'ICANN, tramite una serie di organizzazioni delegate, provvede, quindi, ad assegnare ai richiedenti gli indirizzi "IP" individuati tra quelli disponibili, in maniera permanente oppure in maniera temporanea.

Gli "IP" privati, invece, possono essere definiti delle classi di indirizzi, riservati alle reti locali, utilizzabili da chiunque, e assegnati per ridurre la richiesta di indirizzi "IP" pubblici.

Pertanto, una rete locale che utilizza gli "IP" privati, per essere collegata alla rete Internet, deve utilizzare il dispositivo NAT (Network Address translation).

Il NAT è un servizio che permette a più dispositivi di condividere un unico indirizzo “IP”, potendo così mettere in comunicazione diverse reti.

Gli indirizzi “IP” dinamici provengono da un gruppo predefinito e, sono assegnati, in modo dinamico e casuale, dal server presente nella sottorete.

Per esempio, gli Internet Service Provider (ISP) utilizzano un numero di indirizzi “IP” dinamici, assegnabili per una vasta clientela, facendo leva sul fatto che non tutti i clienti saranno connessi nello stesso momento, e che i loro dispositivi effettuano accessi temporanei.

Gli indirizzi “IP” statici sono utilizzati per identificare dispositivi semi-permanenti con indirizzo “IP” permanente (come nel caso di server e stampanti di rete etc.., che utilizzano questo metodo di indirizzamento).

Il MAC ADDRESS (Media Access Control), è conosciuto anche come indirizzo fisico, indirizzo Ethernet o indirizzo LAN, composto da 12 cifre decimali (dove i primi sei identificano il produttore), ed assegnato, in modo univoco, dal produttore a ogni scheda di rete Ethernet prodotta nel mondo, modificabile, tuttavia, a livello software, al fine di essere utilizzato dai computer, per comunicare nelle reti locali.

Per conoscere il proprio indirizzo “IP” interno che il modem o router assegna al personal computer, nei sistemi operativi “Microsoft Windows”, è sufficiente aprire una “shell” (Prompt dei comandi) digitando “cmd” nella casella di ricerca premendo poi “invio”, all’apertura scrivere il comando “ipconfig” (es. IPv4 192.168.1.4).

Nel caso in cui il comando “ipconfig” non fosse già installato sul sistema, si deve eseguire un doppio click sul file “suptools.msi”, nella cartella/support/tools, nel

CD di installazione.

Attraverso il comando “ipconfig/all” oltre a indirizzo IP, maschera di sottorete e indirizzo IP del gateway, si possono verificare le seguenti informazioni:

Indirizzo fisico: si tratta dell’indirizzo MAC della scheda (identificativo univoco della scheda); Indirizzo IP del DHCP server (con DHCP abilitato) e Indirizzi IP dei server DNS.

Il comando "ipconfig " rappresenta un’ interfaccia di configurazione a riga di comando ovvero un’utilità per l'amministrazione del sistema di rete in Unix/Linux . Esso viene utilizzato per la visualizzazione di informazioni di configurazione di rete corrente, la creazione di un indirizzo IP, maschera di rete o indirizzo broadcast per un'interfaccia di rete, creando un alias per l'interfaccia stessa, la creazione di indirizzo hardware e attivare o disattivare le interfacce di rete.

Nei sistemi operativi “Mac Os X” si può conoscere l’indirizzo “IP” portandosi nel pannello Network in Preferenze di Sistema (Mela > Preferenze di Sistema > Network), selezionando poi la connessione di cui vuoi conoscere l'indirizzo IP agendo sul menu a discesa “mostra”. Anche in questo caso si può agire da terminale utilizzando il comando “ipconfig”.

Mentre, con tutti i sistemi operativi è possibile verificare le informazioni riguardo all’IP pubblico, assegnato al “router” e che identifica il pc all'interno del Web”, all’interno del pannello di configurazione dello stesso “router”. In ogni caso è altresì possibile visualizzare il proprio indirizzo “IP” pubblico attraverso siti internet tipo: “http://www.mostraip.it” oppure http://www.indirizzo-ip.com, sito quest’ultimo che permette di ottenere ulteriori informazioni attraverso la consultazione della banca dati RIPE NCC, che rappresenta uno dei cinque Regional Internet Registry (RIR) e che fornisce l'allocazione delle risorse Internet,

servizi di registrazione e le attività di coordinamento che supportano il funzionamento di Internet a livello globale. Tale banca dati, permette di verificare qualsiasi indirizzo pubblico digitato ed è raggiungibile direttamente all'indirizzo "https://apps.db.ripe.net/search/query.html#resultsAnchor".

8.2) HACKER

Gli "*Hackers*", sono esperti informatici che mettono in rete il loro contributo per favorire lo sviluppo di un software, confidando nel principio della reciprocità, al quale sono legati, all'interno della comunità di appartenenza, strutturata intorno ai principi di un'organizzazione sociale informale, costruita intorno ai network informatici.

A differenza di come si crede, hacker è anche colui che penetra nei sistemi, non per fare danni, ma per il solo gusto di sapere e magari scoprire problematiche nei sistemi software, per il solo gusto di farlo, segnalando poi il fatto al fine di determinare la soluzione del problema.

Eric Raymond definisce un hacker colui che la cultura hacker riconosce come tale.

Con l'espressione "cultura o etica hacker", il finlandese Pekka Himanen definiva la caratteristica culturale dell'informazionalismo.

Gli "hackers" moderni, sono forti sostenitori dei concetti di "*software libero*" e di "*open source software*", poiché accedendo ai "*codici sorgente*" dei software, li migliorano e li adattano ad altri progetti.

Il movimento hacker"*open source*" ha contribuito, strutturalmente, al progresso di Internet, per aver condiviso in rete gli sviluppi tecnologici.

Il movimento hacker per il "*software libero*" nasce per la lotta in difesa dell'apertura

del “codice sorgente” del sistema operativo, potente ed innovativo, “Unix”.

Pertanto, si può affermare che l’input fornito dalla cultura hacker al sistema internet è diventato la base per il suo continuo aggiornamento tecnologico.

8.3) I CRACKERS

I “Crackers”, invece, a differenza degli “hackers”, sono esperti informati irrequieti, ansiosi di crackare codici, penetrare illegalmente nei sistemi, di portare il caos nel traffico informatico.

I “Crackers” e altri generi di “cyber” sono respinti dalla cultura “hacker” e sono definiti, da questi ultimi, sottoculture di un universo “hacker”, più ampio e in genere non destabilizzante.

I “crackers”, in definitiva, sono coloro che compiono atti di pirateria informatica a scopo di lucro.

8.4) MALWARE

Il termine “*Malware”*, è l’abbreviazione di “*malicius software*”; si tratta di programmi che costituiscono un grave pericolo per la sicurezza informatica del sistema.

Il “*Malware*” indica, inoltre, un qualsiasi software, creato con il solo scopo di causare un danno ad un computer, ai dati degli utenti del computer o a un sistema informatico, su cui viene eseguito.

In sintesi, sono dei programmi che, dopo essere stati installati o eseguiti in un sistema informatico o telematico, lo danneggiano, in tutto o in parte, o ne modificano i dati o i

files contenuti, contro la volontà degli utilizzatori del computer.

Succede che, l'accesso, non autorizzato, di detti programmi, c.d."*Malware*", al sistema operativo della macchina ospite, all'insaputa dell'utilizzatore, è causa di numerosi danni, quali:1) sottrazione di dati sensibili dal sistema operativo del computer; 2) appropriazioni di applicazioni di navigazioni in rete, ovvero di account di posta elettronica, per inoltrare attacchi informatici ad altri computer.

Ne consegue, quindi, che, un soggetto, detto "botmaster", può sfruttare i sistemi operativi compromessi dal software appositamente creato ed eseguito sulla macchina ospite, all'insaputa dell'utilizzatore, per scagliare attacchi distribuiti, del tipo "distributed denial of service (DDoS)", contro qualsiasi altro sistema in rete.

Questa rete, di "virus" invisibili,creata dai "botmasters", con la presenza di particolari file o impostazioni del sistema, all'insaputa sia degli utenti sia dei programmi antivirus, installati sul computer, si chiama "*botnet*"; mentre i computers infettati da questi "*virus*" invisibili sono detti "*zombie bot*".

Si distinguono molte categorie di programmi c.d. "*malware*", di seguito si riportano i più comuni:

a) "*Virus*": sono programmi che si diffondono, copiandosi, all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni qualvolta il file infetto viene aperto;

b) "*Worm*": è un programma informatico dannoso che modifica il sistema operativo della macchina ospite, in modo da essere eseguito automaticamente, e tentare di replicarsi, utilizzando Internet. Il Worm carpisce, dal programma di posta elettronica del sistema informatico o

telematico ospite, l'elenco dei contatti, e invia, a questi ultimi, delle mail con l'allegato infetto, con lo scopo di diffondersi, una volta aperto;

c) "*Spyware*": software che accumula informazioni dal sistema per trasmetterle ad un destinatario interessato e/o terzi;

d) "*Adware*"(*advertising-supported software):* sono programmi che, automaticamente, riproduce, visualizza e scarica pubblicità su un computer durante l'uso.

Nella categoria degli "*Spyware*" rientrano i "*Cookies", che sono file* di testo, innocui, che contengono dati e informazioni di accesso ad un determinato sito appena visitato, e serve per facilitare e velocizzare un futuro accesso al sito web medesimo.

e) *"Trojan horse" (cavallo di Troia):* è un software dannoso che assume le sembianze di un'applicazione utile, ma che, in realtà, danneggia il computer o ruba dati una volta installato. I "*Trojan*" differiscono dalla categoria dei "*Virus*", in quanto non si replicano, ma hanno un duplice scopo: di danneggiare, in tutto o in parte, il sistema informatico, compromettendone così la sicurezza; di aprirvi un accesso, permettendo da remoto, il più assoluto controllo del sistema operativo, per modificarne e/o carpirne i dati o *file* ivi contenuti.

f) "*Keylogger"*:sono programmi che, una volta all'interno di un sistema informatico, intercettano e registrano tutto ciò che un utente digita su una tastiera o che copia e incolla, rendendo, così, possibile il furto di *password* o di dati.

I dati sottratti in locale sul personal computer, e trasmessi ad un "*hacker*", in remoto, possono riguardare: a) dati sensibili, b) dati di accesso a servizi

bancari, c) carte di credito, d) posta elettronica;

g) *"Scarware":* sono programmi che ingannano l'utente facendogli credere di avere il proprio personal computer infetto, allo scopo di fargli installare dei particolari "*Malware*"*,* chiamati in gergo "*rogue antivurus"* caratterizzati per essere degli antivirus veri e propri, a pagamento. Rientrano nella stessa categoria i "*RogueAntispyware*", che si mostrano quali finti programmi per la sicurezza del computer, spingendo gli utenti ad acquistare una licenza del programma;

h) "*Rabbit*" detti anche bacteria o wabbit: sono software che esauriscono le risorse del computer creando copie di se stessi;

i) "*Dialer*": programmi che si occupano di gestire la connessione ad Internet tramite la normale linea telefonica;

l) "*Rootkit":* software che nascondono, sia all'utente che ai programmi antivirus, la presenza di particolari *file* o impostazioni del sistema.

8.5) IL DEFACEMENT

Il "*Defacement*" (letteralmente: deturpare, sfregiare,sfigurare), è una forma di atto vandalico virtuale, compiuta nell'ambito della sicurezza informatica.

Il "*Defacing"*consiste in una operazione fatta, da remoto, da un "*hacker*", per cambiare, illecitamente, la "*home page*" di un sito "*web*" (la sua "*faccia*"), o per modificare, in tutto o in parte, sostituendole, una o più pagine interne, all'insaputa dell'amministratore del sito, inserendovi immagini, testi, video, propaganda, etc..

Quindi, in definitiva, le motivazioni che spingono l'"*hacker*" a compiere tali azioni vandaliche, sono da ricercare in molteplici fattori, quali: dimostrazione di abilità,

motivazione ideologica o partitica.

Gli “hacker”, per ottenere i permessi di accesso in scrittura al sito sfruttato, utilizzano i “*bugs*” (bachi), presenti nel software di gestione del sito o nei sistemi operativi. Il “*bug*”, in informatica, indica un errore nella scrittura di un programma software.

8.6) E-MAIL

Le “*E-Mail*” (dall’inglese: electronic mail) sono un servizio Internet con il quale ogni utente, abilitato, utilizzando un computer o altro dispositivo elettronico connesso in rete, attraverso un proprio account di posta registrata presso un provider di servizio, può inviare e ricevere messaggi.

Le “*E-Mail*” possono essere paragonate alle lettere tradizionali, si differenziano in quanto, rappresentando la controparte digitale ed elettronica, non si servono della tradizionale penna e carta per scrivere messaggi, che arrivano, dal mittente al destinatario, in pochi secondi/minuti, ma utilizzano il sistema informatico, connesso alla rete Internet.

In definitiva, le “E-Mail” costituiscono una rivoluzione nel modo di inviare e ricevere posta, con la possibilità di allegare qualsiasi documento e immagine digitale. L’invio indiscriminato di numerose “*E-mail*” è detto “spamming”, ed è illegale per la legge italiana.

Si consiglia, quando si crea un indirizzo “*E-Mail*”, di adottare le precauzioni dovute, al fine di proteggere la propria identità personale da indebite interferenze nella vita privata.

A tal fine, sarebbe opportuno procedere con cautela ogni qualvolta si ricevono messaggi, con allegati, anche non visibili, da sconosciuti, sul proprio indirizzo di posta elettronica, i quali potrebbero contenere software pericolosi, tipo "*worm*", "*virus*", "*trojan*".

Si consiglia, inoltre, di evitare di rispondere ai loro messaggi ricevuti, in quanto si potrebbe, involontariamente, far conoscere ad estranei il proprio indirizzo di posta elettronica.

Si sconsiglia, in ultimo, nel dubbio, di inviare e far conoscere ad estranei, a mezzo di posta elettronica, i propri dati personali, e/o fornire informazioni private, foto, video e quant'altro in vostro possesso.

8.7) SPAMMING

Lo "*Spamming*" consiste nell'invio di numerosi messaggi, sia sulla posta elettronica, sia sui forum o sulle chat, senza il consenso del destinatario.

Di solito, si inviano messaggi pubblicitari e/o commerciali, che possono intasare la casella di posta elettronica, con pregiudizio per il suo regolare funzionamento.

Nelle chat o nei forum, l'invio di "*Spam*", rende difficoltosa la conversazione o la discussione tra utenti.

Il termine "Spamming"trae origine da uno sketch comico britannico, del gruppo MontyPython, ambientato in un locale, nel quale la cameriera proponeva, in maniera petulante e fastidiosa ai clienti, solo pietanze a base di "*Spam*" (un tipo di carne di maiale in scatola).

Si pensa, che il primo "*Spam*", detto anche "*junk-mail*", che significa

letteralmente posta spazzatura, sia stato lanciato via "e-mail" nel maggio del 1978, per pubblicizzare un nuovo prodotto.

Quindi scopo principale dello "Spammer", soggetto autore dei messaggi "Spam", è quello di inviare messaggi identici a migliaia di indirizzi *e-mail,* ciò è causa di uno dei maggiori fastidi di Internet.

Pertanto, l'utente, vittima di questi fastidiosi messaggi pubblicitari, non deve rispondere alle *e-mail* di posta spazzatura, e richiedere la cancellazione dai loro elenchi.

Il Garante della Privacy, ha chiarito gli aspetti normativi in materia di "Spamming", e all'art 130 del d. lgs. n.196 del 2003, (codice per la protezione dei dati sensibili, comunemente detto codice privacy), rubricato "comunicazioni indesiderate", vieta l'invio di posta elettronica ai fini commerciali, per la vendita diretta o facendo ricerche di mercato, camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i propri diritti.

8.8) PHISHING

Il "Phishing" è una vera e propria truffa realizzata attraverso la rete Internet.

Esso consiste in una attività illegale posta in essere da un malintenzionato, il quale invia all'ignara vittima delle false *e-mail* (c.d."*esche*"), che simulano la grafica di siti bancari o postali,cercando, in tal modo, di convincere la stessa vittima a fornire informazioni personali sensibili.

In definitiva, l'aggressore, ponendo in essere tale attività illegale, cerca di ottenere dalla vittima informazioni sulla propria *password* di accesso al conto

corrente bancario, o il proprio numero della carta di credito.

L'attività illegale del malintenzionato, finalizzata alla truffa informatica,presenta la seguente metodologia di attacco:

a) invio di false *e-mail* all'utente, contenenti le c.d. "*esche*", consistenti in messaggi che simulano la grafica di siti bancari o postali;

b) invito, sempre rivolto all'utente, a validare i propri dati di accesso al servizio, in conseguenza del verificarsi di problematiche del proprio conto corrente bancario o postale, che possono essere di varia natura (come ad. es.: indicazione che in caso di non accesso l'account verrà sospeso o bloccato);

c) invito rivolto all'utente a collegarsi a un determinato sito cliccando su un *link* indicato nel messaggio;

d) il *link* rimanda ad un sito *web,* apparentemente simile a quello ufficiale della banca, ma in realtà è un sito fittizio, gestito dal truffatore, e viene chiesto all'utente di inserire i propri dati personali sensibili di accesso in rete (*username e password*). Tali dati saranno memorizzati su un server gestito dal *phisher*, e, successivamente, utilizzati dal malvivente per compiere operazioni illecite. In questo preciso momento, apparirà all'utente un avviso, che per problemi tecnici, non potrà accedere al servizio bancario, oppure che l'account sarà momentaneamente bloccato.

Questi truffatori per camuffare l'indirizzo *web* fasullo, fanno comparire nella stringa "*URL*" (*Uniform Resource Locator*) il nome vero del servizio a cui l'utente vorrebbe accedere, nascondendo quello a cui, in realtà, si verrà indirizzati, sostituendolo con caratteri esadecimali o codice "*ASCII*" o formato "*IP*"(numeri), seguiti prima dal simbolo @.

La chiocciola posta fra l'indirizzo vero e quello fasullo, per impostazioni del *browser*, fa sì che, lo stesso riconosce solo l'indirizzo posto dopo il simbolo.

Occorre ricordare, quindi, che nessun istituto di credito, nessuna finanziaria, nessun Ente, presso cui si è registrati *on-line*, chiederà i dati personali, a mezzo di posta elettronica, per registrarsi e loggarsi, per poter accedere ai loro servizi.

Pertanto, l'utente, in caso di dubbio sulla genuinità del messaggio ricevuto, farebbe bene a diffidare dei *link* che rimandano ad un sito web, apparentemente simile a quello ufficiale del proprio istituto di credito, per non incorrere in una truffa, e, sarebbe buona cosa, prima di accedere alla *home page* conosciuta ed utilizzata, abitualmente, nel *browser,* contattare il fornitore del servizio.

Si consiglia, inoltre, di installare sul proprio dispositivo un buon programma "*anti-virus", "anti-spam", "firewall"*, costantemente aggiornato, e di verificare, sempre, che la trasmissione dati, per le operazioni c.d. "*a rischio*", avvenga con protocollo cifrato, nonchè, controllare, che l'indirizzo "*URL*" sia, effettivamente, quello a cui si desidera accedere.

8.9) PHARMING

Il "*Pharming*" richiama il modello di "*Phishing*", è una tecnica di "*craking*", utilizzata per ottenere l'accesso ad informazioni personali e riservate.

Tecnicamente, l'utente viene ingannato e portato a rilevare, inconsapevolmente, a sconosciuti, i propri dati sensibili, relativi al proprio numero di conto corrente, alla propria *password*, etc..

La metodologia di attacco del "*Pharming*" è, dunque, analoga a quella del "*Phishing*", e

consiste, principalmente, nel far collegare l'utente, ad un sito, apparentemente, identico all'originale, ma, in realtà, creato allo scopo di carpire i propri dati personali.

Accade, in seguito, che ogni qual volta l'utente digita sul proprio browser l'indirizzo di una pagina *web, come quella d*ella propria banca, anziché essere tradotto, automaticamente, dai calcolatori, in un indirizzo *IP* numerico, per reperire, nella rete *Internet*, il percorso per raggiungere il *server-web* corrispondente a quel dominio,viene, inconsapevolmente, reindirizzato ad un server trappola, reperibile all'indirizzo IP, inserito dal *craker*, ovvero su un sito clone dell'originale, appositamente predisposto dal soggetto malintenzionato, apparentemente simile a quello vero, per carpirgli le informazioni.

8.10) FILE SHARING

Il "*File sharing*" consiste nella condivisione di *file* all'interno di una rete di calcolatori.

I programmi di "*File sharing*" che, come detto, consentono di trasferire file da un computer ad un altro, su Internet o su reti aziendali Intranet, possono essere del tipo "client-server" (cliente-servente) o del tipo "peer to peer" (pari a pari).

Orbene, nella considerazione che le reti di "*file-sharing"* siano una risorsa di informazioni, sulle preferenze degli utenti e le tendenze di mercato, sarebbe opportuno che i clienti di questi programmi in rete adottassero delle precauzioni per salvaguardare la loro privacy.

Infatti, la possibilità per gli utenti di scaricare (*download*) enormi quantità di dati, espone il proprio personal computer a numerosi rischi di intrusione e minacce

malware, del tipo "*virus", "trojan*", nonché a venire in possesso di materiale indesiderato, in particolar modo utilizzando programmi di condivisione "peer to peer" tipo i software emule o Mirc.

Il "*file sharing*" è reso possibile da appositi programmi installati sul personal computer e lo scambio avviene fra gli stessi utenti connessi al medesimo programma.

Dunque, quando un navigatore di Internet cercherà di collegarsi con altri per condividere file, occorre fare attenzione a ciò che si vuole condividere, perché questi programmi possono portare sia vantaggi che svantaggi, per la presenza di contenuti protetti da diritto d'autore.

Infatti, potrebbe accadere che, l'utente, convinto di portare a termine un download di un determinato *file*, potrebbe scaricare, alla fine, un *file* del tutto diverso da quello desiderato (materiale pornografico, etc..), in tal caso, il sito potrebbe essere oscurato e la rete divenire inoperativa.

Il funzionamento del "*file sharing*" è molto semplice, installato il *software* preposto sul personal computer, e dopo essersi connessi alla rete *Internet*, lo si avvia, consentendo, in tal modo, la connessione a dei server nei quali sono presenti i *file* scaricati, si digita il nome del *file* richiesto, e si inizia la ricerca.

I programmi di "*file sharing*" comunemente utilizzati sono: "*Utorrent*", "*Bitorrent*", *Emule* e il programma di "*Chat Mirc*".

8.11) LE CHATROOM, NEWSGROUP, FORUM, INSTANT MESSAGING

Le "Chatroom" (in inglese, letteralmente stanza delle chiacchiere), sono servizi sia telefonici che per via Internet, e consentono il contatto tra due perfetti

sconosciuti, in un luogo o spazio virtuale, appunto la "*Chatroom*", in cui avviene, in tempo reale, la chiacchierata. Esistono numerosi siti-*web* che offrono il servizio di *chat*, ogni chat può essere suddivisa in stanze, e ciò dipende dall'argomento principale trattato, dalla fascia di età dell'interlocutore.

I messaggi inviati in chat possono essere di dominio pubblico, per tutti gli utenti che si collegano alla "*chat*", ovvero privati, se diretti ad un determinato utente e/o gruppi di utenti; possono, inoltre, essere scritti e/o vocali, e la conversazione può avvenire in videoconferenza.

Ma accade spesso, che molti utenti paragonano l'ambiente virtuale della *chat* alla vita reale, commettendo in tal modo una grave disattenzione, potendo incorrere, fornendo agli anonimi e sconosciuti interlocutori, a volte, informazioni sulla propria vita, a pericoli quali:

1) la sottrazione di dati sensibili e personali, che possono essere, successivamente utilizzati dall'interlocutore, per fini illeciti, con grave violazione della propria privacy;

2) l'installazione e l'esecuzione, da parte dell'interlocutore malintenzionato, dei "*malware*", che si diffondono agli altri utenti collegati alla "*chat*".

E' risaputo, inoltre, che le "*chat*" sono luoghi virtuali in cui prolificano malintenzionati di ogni genere (come, pedofili, molestatori, truffatori, etc..) per adescare, con l'inganno, le potenziali vittime, i quali fingendosi interessati alla problematica trattata, e direttamente coinvolti, riescono ad ottenere, appunto dalla vittima prescelta, numeri di telefono, indirizzi o altri recapiti, utilizzandoli, successivamente per fini loschi.

Ultima raccomandazione per i navigatori di Internet, ma importantissima è quella di non accettare mai di incontrare, personalmente, queste persone.

I “Newsgroup”, “*Forum*” sono spazi virtuali creati a mezzo di programmi chiamati *new-client*, (a volte già integrati nei programmi di posta elettronica o nei principali portali o direttamente offerti dai *provider (ISP),* nei quali è possibile, tra gli utenti della rete, mandarsi e leggere, in tempi reali, messaggi, scambiarsi *file,* discutere. “*Newsgroup*”, “Forum”, si differenziano dalle “*chat*”, per molteplici fattori, tra i quali: mentre nelle “*chat*” non è obbligatoria la registrazione e la conversazione è immediata, nei “*Newsgroup*”, “*Forum*” la conversazione può avvenire anche in momenti diversi ed è obbligatoria la registrazione o una conferma di un indirizzo e-mail, sia per leggere che per inviare messaggi.

Gli spazi virtuali “Newsgroup”, “Forum” richiedono al navigatore in Internet di adottare le dovute cautele, per tutelare la propria privacy.

“L’Instant Messaging” o servizio di messaggistica istantanea (IM), utilizza il sistema di comunicazione sopra descritto “peer to peer” (pari a pari), consentendo l’invio di messaggi, in tempo reale, sia ad altri utenti connessi alla rete, sia a telefoni cellulari.

Anche quando l’utente utilizza questo sistema di messaggistica, deve apprestare le dovute cautele, a difesa dei propri dati personali e sensibili.

8.12) SOCIAL NETWORK

I “*Social Network*” o servizi di rete sociale sono delle piazze virtuali, create da gruppi di individui connessi tra loro da diversi legami sociali, in cui è possibile registrarsi e creare un proprio profilo personale che può essere, in tutto o in parte, pubblico, con all’interno inserita una lista di contatti. Lo scopo di questi servizi di rete sociale è quello di rinsaldare, attraverso queste piazze virtuali,

amicizie con persone con le quali si erano persi i contatti, ovvero ampliare la propria sfera di contatti o ambito di conoscenze.

Con la registrazione a questi social network, l'individuo/navigatore immette in rete i propri dati personali e sensibili, visibili a tutti gli altri utenti/navigatori di Internet, comprese le proprie immagini. Così facendo, l'utente, rischia, che altri individui/navigatori, malintenzionati possano utilizzare, illecitamente e senza il suo consenso, i propri dati personali.

Pertanto, sarebbe opportuno adottare le seguenti precauzioni a tutela della propria privacy:

a) proteggere, nelle impostazioni del social network, il proprio profilo;

b) inserire, nelle liste personali, solo i contatti "sicuri";

c) fornire le minime e strette informazioni personali e sensibili;

d) limitare la pubblicazione di foto e video personali (foto e i video divulgati in rete possono essere utilizzati da terzi e diffusi nella rete per creare falsi profili).

8.13) E-COMMERCE

"L'e-commerce" (commercio elettronico), è uno dei principali servizi offerti dalla rete Internet, in continua espansione, e consiste nella commercializzazione di beni e servizi tra produttore e consumatore, tramite *Internet*, nonché l'insieme delle transazioni commerciali.

Le problematiche connesse a questo servizio, per chi vende e per chi acquista, sono molteplici e attengono la protezione dei dati personali in rete, la globalità del fenomeno, la genuinità delle informazioni scambiate, la sicurezza nei pagamenti.

Per acquistare *on-line* occorre:

1) accedere ad un determinato sito *web* dedicato al commercio elettronico, a volte è richiesta la registrazione;

2) scegliere il prodotto desiderato;

3) procedere al pagamento, con carta di credito o servizi intermediari.

I rischi, connessi all'utilizzo di questo servizio in rete, sono: a) il bene acquistato non arriva mai a destinazione, o giunge danneggiato, o non funzionante; b) il bene acquistato presenta caratteristiche diverse da quelle pubblicizzate dal rivenditore; c) il titolo di pagamento utilizzato è stato, indebitamente, usato contro la volontà e all'insaputa del titolare.

Il rischio per il venditore è quello di non ricevere mai nessun compenso.

8.14) ANNUNCI EFFETTUATI A VOSTRO NOME

Capita spesso che ignoti, per le più disparate motivazioni, possano effettuare inserzioni, su siti di "compra-vendita" e di "incontri", spendendo il vostro nome, e a vostra insaputa.

Lo scopo è, sostanzialmente quello di eludere, nei siti "compra-vendita", la reale identità dell'inserzionista che si serve della vostra identità e/o utenza telefonica, a vostra insaputa, per compiere truffe *on-line*.

Si consiglia, quindi, di effettuare, periodicamente, sui motori di ricerca "Google" e "Yahoo", delle verifiche con i vostri dati personali e sensibili, al fine di accertarsi che non siano utilizzati da terzi, illecitamente e senza il vostro consenso, sui suddetti motori di ricerca Internet, per la vendita di oggetti in rete.

Se la ricerca dà esito positivo, si consiglia di chiedere, immediatamente, la rimozione dei vostri dati dall'annuncio fatto da terzi, ai gestori del sito *web*, e, se del caso, qualora i vostri dati non fossero rimossi, denunciare il fatto alla Polizia di Stato, dopo aver copiato la stringa *URL* e la pagina dell'inserzione.

I siti di "Incontri" hanno, invece, uno scopo diffamatorio. Infatti, spesso, le inserzioni fatte pubblicare da terzi, a vostra insaputa, contengono non solo i vostri dati, personali e sensibili, ma, gli stessi, sono corredati da vostre foto personali, reperibili facilmente su "*facebook*".

Pertanto, anche in questo caso, si consiglia di denunciare il fatto alla Polizia di Stato, sempre dopo aver richiesto di rimuovere l'annuncio diffamatorio dal servizio clienti che gestisce il sito-web.

8.15) RETI "WI-FI" LIBERE

Il termine "*Wi-Fi*" indica una tecnologia in grado di consentire ai terminali di utenza di collegarsi fra loro attraverso una rete locale, in maniera "Wireless" (WLAN), allacciata alla rete Internet, e, così, usufruire dei servizi di connettività offerti da un "ISP" (Internet Service Provider).

Spesso accade, che molti utenti della rete Internet, sia per buona fede, sia per incompetenza in materia, non proteggano con una password la loro connessione "Wi-Fi", oppure non cambiano la password predefinita del loro router che è facilmente individuabile attraverso appositi software.

In tal caso, può capitare che la rete Internet di questi utenti, priva di protezione, può essere oggetto di attacco da parte di terzi, che trovandosi nelle loro vicinanze, con un

qualsiasi dispositivo di accesso ad Internet "Wi-Fi", si connettono al loro terminale, e a loro insaputa, lo possono utilizzare anche per fini illeciti.

Quindi, per evitare il verificarsi della descritta situazione, è necessario che tali utenti, in buona fede e principianti, non solo proteggano con un'appropriata password la connessione "Wi-Fi", ma debbono astenersi dal comunicare, ad estranei, i loro dati di protezione.

8.16) FALSA ASSUNZIONE DI LAVORO

La falsa Assunzione di Lavoro, costituisce uno dei tipi di truffa, più comuni, *on-line,* posta in essere da alcuni siti, i quali sul loro portale di ricerca lavoro inseriscono inserzioni di false assunzioni di lavoro, come ad esempio, l'assunzione di personale da inserire nella loro azienda, per controllo qualità di prodotti acquistati *on-line*.

La tecnica posta in essere da questi siti, e in cui si sostanzia la promessa di falsa assunzione, è la seguente: dopo aver ricevuto le numerose domande dai malcapitati utenti, in cerca di occupazione, spediscono a questi ultimi uno pseudo contratto di lavoro, e contestualmente richiedono, ai medesimi utenti, l'invio di documenti personali e le coordinate bancarie, su cui accreditare le eventuali future provvigioni, con la promessa di formale invio, a mezzo corriere, presso la loro abitazione, del materiale necessario per svolgere il lavoro (personale computer, macchine digitali).

Successivamente, l'azienda, datore di lavoro, si riserva di comunicare agli utenti, in disperata ricerca di lavoro, gli indirizzi del presunto cliente finale, al quale rispedire il prodotto lavorato, sempre a mezzo corriere.

C'è da dire che spesso il presunto cliente finale, quasi sempre domiciliato all'estero, ha effettuato numerose clonazioni di carte di credito, appartenenti a persone ignare, che, si sono accorte di numerose movimentazioni sospette effettuate con la loro carta di credito ed hanno quindi provveduto a sporgere la relativa denuncia alla Polizia di Stato.

L'attività di monitoraggio della Polizia di Stato ha consentito di appurare, dall'estratto conto, pagamenti *on-line* effettuati, con la carta di credito duplicata, per acquisto di prodotti su siti *Internet* di famose aziende, fatturati a nome del malcapitato utente, vittima della clonazione.

Presumibilmente, avviene che il sito iniziale che ha proposto e organizzato falsi lavori da casa, sicuramente complice del c.d. cliente finale o magari sono le stesse persone, effettua acquisti su portali di aziende serie, utilizzando carte di credito clonate, comunicando come dati di fatturazione ed invio quelli dei malcapitati utenti disoccupati.

Ovviamente il "giochino" dura poco, in quanto gli utenti che falsamente sono occupati dall'azienda per svolgere un lavoro di controllo di qualità di prodotti acquistati on-line, non saranno mai pagati, ed inoltre, inspiegabilmente, il sito in questione non sarà più raggiungibile e/o scomparirà, con l'interruzione di qualsiasi tipo di comunicazione.

Il malcapitato utente, può rischiare di incorrere in gravi conseguenze penali, pertanto, è buona cosa, che lo stesso conservi con cura ogni comunicazione mail, nonché il contratto di lavoro spedito dal sito truffaldino, e quant'altro possa servire come prova, per dimostrare la propria buona fede.

Il consiglio è quello di effettuare alcune ricerche in rete, attraverso i più grandi

siti di motori di ricerca (https://www.google.it/, https://www.bing.com/, https://it.yahoo.com), al fine di verificare se esistono blog di discussione relativi al sito in esame, prima di rispondere agli annunci fatti di false promesse di lavoro.

8.17) CARTE DI PAGAMENTO (BANCOMAT E LA CARTA DI CREDITO-DEBITO)

La "*carta di debito*" o "*Bancomat*", è una carta di pagamento che prevede l'addebito immediato sul conto corrente del titolare delle somme spese, per mezzo della carta, presso gli esercizi commerciali o prelevate presso gli sportelli automatici bancari.

Le "*Carte di Credito-Debito*" sono, inoltre, il mezzo più diffuso per il pagamento di beni e servizi acquistati dai clienti *on-line*.

Prima di effettuare un acquisto *on-line* è bene scegliere con accuratezza il negozio *on-line,* per non incorrere nel pericolo che la "*Carta di Credito-Debito*" possa essere clonata da malintenzionati o subire la cattura dei codici di accesso.

Pertanto, occorre diffidare delle offerte a prezzo stracciato, in quanto costituiscono il primo campanello d'allarme,per coloro che sono intenzionati ad acquistare on-line, sulle possibili affidabilità di un rivenditore, per non incorrere in una, probabile, truffa.

Dunque, prima di procedere all'acquisto di beni e servizi on line, è bene seguire le seguenti regole, che si consigliano, quando si fa shopping on-line:

1) prendere informazioni sull'affidabilità del rivenditore;

2) leggere attentamente le condizioni generali del contratto di acquisto;

3) accertarsi che le transazioni siano effettuate in tutta sicurezza, ovvero su connessione protetta. A tal riguardo, sarebbe opportuno che sul browser del computer dell'acquirente fosse installato un anti-virus, aggiornato, e/o un "firewall", per bloccare eventuali furti di informazioni;

4) verificare, con attenzione, le caratteristiche del prodotto che si intende acquistare;

5) prestare attenzione ai pagamenti anticipati;

6) ricordarsi di stampare e conservare con cura tutta la documentazione relativa all'acquisto, anche per usufruire delle garanzie o del diritto di recesso dal contratto;

7) In caso di ulteriori dubbi sarà possibile controllare la validità della partita iva comunitaria presente sul sito e-commerce nonché la compatibilità dei dati riportati sulla stessa con quelli della denominazione aziendale presente sul sito in questione. La verifica potrà essere effettuata attraverso il seguente indirizzo: http://www1.agenziaentrate.gov.it/servizi/vies/vies.htm?p=&s=IT;

8) Valutare l'opportunità di sfruttare nuovi mezzi di pagamento che presentano minori rischi, ad esempio l'uso di carte di credito ricaricabili o l'utilizzo del sistema di pagamento paypal (https://www.paypal.com/it);

9) E' opportuno ricordare che su tutti i sistemi operativi microsoft è disponibile gratuitamente il software antivirus "Microsoft Security Essentials", scaricabile direttamente dal sito della casa madre che, ricordiamo, va tenuto costantemente aggiornato. Tale software è già integrato nel sistema operativo a partire dalla distribuzione windows 8, pertanto in questo caso non necessita di installazione. Segue il link per scaricare l'antivirus MSE: "http://www.microsoft.com/it-it/security/pc-security/mse.aspx";

10) Spesso accade che installando dei software freeware (completamente gratuiti) o trial (in prova), contestualmente vengono installati software accessori ai quali il soggetto consente involontariamente l'accesso al sistema, magari per scarse competenze nella lingua inglese o perché non procede con l'installazione personalizzata che consente di scegliere il software necessario. Nella gran parte dei casi questi software sono costituiti da adware, barre degli strumenti, programmi potenzialmente indesiderati (pup) e hijacker del browser dal computer che spiano le abitudini dell'utilizzatore della rete internet. L'internauta noterà che la prima pagina di apertura del browser (internet explorer, mozilla firefox, chrome, safari etc.) che si utilizza è cambiata e/o vi sono delle barre degli strumenti accessorie rispetto a quelle standard. Sicuramente sarà necessario fare una scansione con apposito antivirus del sistema ma, purtroppo, sui sistemi windows spesso non si risolve il problema. Pertanto, si consiglia l'uso di programmi specifici tipo "adwcleaner" raggiungibile all'indirizzo:

    "https://toolslib.net/downloads/viewdownload/1-adwcleaner".-

Esistono servizi di sicurezza messi a disposizione del cliente dalle società emettitrici delle carte di credito, quali il servizio di SMS-Alert. Tale dispositivo avverte il cliente, con l'invio di un SMS sul proprio cellulare, delle operazioni eseguite con la propria "Carta di Credito-Debito".

Mentre, il servizio "bankpass" ,che inerisce le transazioni on-line, non è altro che un "portafoglio elettronico" creato dall'Istituto bancario e collegato alla carta di pagamento in possesso del cliente, al quale è assegnata una *userid* e *password*.

Altro servizio offerto dagli istituti di credito ai loro clienti, per garantire loro la massima sicurezza nella movimentazione di somme di danaro *on-line*, con la

carta in loro possesso, è l'assegnazione di un numero di carta virtuale, collegato a quella reale, utilizzabile una sola volta.

Si rinnova il consiglio di prestare particolare attenzione quando si fa shopping *on-line*e, soprattutto, che la "*Carta di Credito-Debito*" non venga mai usata come strumento di pagamento su siti di natura dubbia.

Infatti, gli utenti, navigando su questi siti sospetti, spesso incorrono nel rischio che i dati presenti sulla propria carta sono rubati e utilizzati da malintenzionati, per effettuare transazioni a loro insaputa.

Si ricorda che la truffa classica, effettuata tramite Internet, è il c.d. "*phishing*", già in precedenza ampiamente illustrato, ovvero l'invio di messaggi pubblicitari, che arrivano via posta elettronica o che si trovano su siti *Internet*, di dubbia origine, che pubblicizzano improponibili sconti su prodotti di moda (come *smartphone, tablet*, etc..).

In ultimo, quando si eseguono operazioni con il circuito "*Bancomat*", prima di digitare il proprio codice *PIN*, si consiglia di accertarsi che la tastiera, la fessura di introduzione, in cui inserire la propria "Carta di Credito-Debito",presente su detto circuito "*Bancomat*" (ATM), non mostrino segni di manomissioni o dispositivi tipo "skimmer", e/o telecamere.

Inoltre, è opportuno non consegnare la propria "*Carta di Credito-Debito*" a nessuno, e durante l'utilizzo *on line* della detta carta di pagamento, accertarsi che il proprio browser, che consente la connettività in Internet, utilizzi un sistema di protezione del flusso dati, contro virus, trojan, spyware, keylogger.

Va ricordato che il traffico effettuato mediante il browser si basa sul protocollo HTTP (Hyper Text Transfer Protocol), che ha l'unico compito del trasferimento delle informazioni ad alta velocità tra il mittente ed il destinatario attraverso il

protocollo TCP (Transmission Control Protocol) sulla porta 80 del computer (ad. esempio http://www.amazon.it/).

Tutti i siti di e-commerce (banche, PayPal, Ebay, Poste Italiane etc.), nel momento in cui si dovranno inserire i dati per il login o per il pagamento utilizzano il protocollo HTTPS (Secure HyperText Transfer Protocol) il quale impiega, oltre ad i protocolli TCP e HTTP, un ulteriore livello che si occupa della crittografia ed autenticazione dei dati trasmessi che viene denominato SSL (Secure Sockets Layer). I dati transitano sulla porta 443 anziché 80 (ad. esempio https://www.amazon.it/).

L'HTTPS rende univoci i mittenti ed i rispettivi destinatari delle informazioni mentre il protocollo SSL cripta i dati, in entrata come in uscita. Tale operazione richiede che il proprietario di un sito web acquisti un certificato da un'autorità di certificazione, come Verisign (http://www.verisign.it/) o lo generi in proprio.

Web browser quali Mozilla Firefox e Chrome utilizzano il protocollo https ovunque (se non abilitato lo si può fare attraverso le opzioni del plugin: Strumenti, Componenti aggiuntivi, httpsEverywhere).

8.18) I DIALER

Il "*Dialer*"è un programma per personal computer, che, tramite la linea telefonica PSTN o un collegamento ISDN, crea una connessione ad Internet, ad un'altra rete di calcolatori o ad altro computer.

Questi programmi, che consentono di accedere a servizi a tariffazione speciale, spesso nascondono frodi o truffe, in quanto, all'insaputa dell'utente, possono

alterare i parametri di connessione a Internet, impostati sul proprio computer. In tal modo, operando sul numero telefonico dell'utente medesimo, e sostituendolo con un numero a pagamento maggiorato, su prefissi internazionali satellitari o speciali, possono indirizzare la connessione Internet verso numerazioni c.d. "a valore aggiunto".

Talora accade che i "Dialer", che non sono veri e propri virus, siano difficili da identificare anche attraverso l'uso dei migliori anti-virus che ne blocchino il funzionamento, tentando di accedere, piuttosto che ad un singolo nodo (il personale computer di chi ha la super-bolletta), all'intera rete di un operatore di telefonia, per collegarsi poi, con virus, a tutti i nodi della rete.

Accade di frequente, allora, che l'utente, componendo, semplicemente, il numero dell'operatore telefonico, coinvolto dall'accesso, sopra descritto, può trovarsi il "Dialer" sul computer, senza aver visitato nessun sito, che offre servizi a tariffazione speciale.

A tal proposito, si ricorda che l'operatore telefonico provvede ad aggiornare, periodicamente, l'antivirus aziendale, per prevenire illecite intrusioni, ma, lo stesso, non ha nessun obbligo di comunicare al cliente l'esistenza di un pericolo proveniente da un "bug" (errore nella scrittura di un programma software), irrisolto, sulla sicurezza della propria rete Intranet.

Quindi, il consiglio che si dà ai navigatori in Internet, è quello di controllare che la connessione predefinita utilizzi il numero fornito dal proprio provider, ed, eventualmente, chiedere la disattivazione dei numeri "a valore aggiunto" (VAS, acronimo di value-added service), al gestore telefonico.

Inoltre, si consiglia, agli stessi utenti, di installare sul proprio personal computer

programmi anti-dialer, che blocchino la connessione ai numeri non espressamente autorizzati.

Il Ministero delle Comunicazioni, in ottemperanza della direttiva Europea n. 97/66 CE, emanata per normalizzare la trasparenza verso gli utenti, per garantire, appunto, l'anonimato di chi chiama, ma non di chi viene chiamato,ha reso difficoltosa l'individuazione del "*Dialer*", con tabulati redatti con le ultime tre cifre non in chiaro.

In tal modo, senza la lista completa dei numeri chiamati, con le ultime tre cifre mancanti o oscurate, non sarebbe stato possibile individuare la causa di bollette particolarmente "salate".

La questione, sopra evidenziata, ha costituito oggetto di intervenuto da parte dell'Autorità Garante per la Privacy con provvedimento del 13 marzo 2008 (Misure in materia di fatturazione dettagliata) pubblicato in Gazzetta Uficiale n. 79 del 03/04/2008).

Infatti tale Organo Collegiale, istituito per la protezione dei dati personali, a far data dal 1 luglio 2008, ha disposto che le compagnie telefoniche emettessero fatture dettagliate in assenza di esplicita richiesta di oscuramento con "asterischi" da parte dell'abbonato, per l'individuazione del dialer, pertanto con le ultime 3 cifre in chiaro e con l'indicazione del numero chiamante.

8.19) PEDOFILIA ON-LINE

La pedofilia, in senso etimologico, significa "amare e sentirsi attratti da bambini e giovanissimi", anche in forma non patologica e del tutto innocua; mentre, dal

punto di vista clinico, rappresenta un disturbo psicologico, rientrante nella categoria delle c.d. "*parafilie*", così come descritto nel manuale diagnostico e statistico dei disturbi mentali (DSM-IV).

La "*pedofilia on-line*", invece, è il comportamento di persone pedofili che utilizzano la rete *Internet* per incontrare altri pedofili, per scambiare materiale pedopornografico e/o adescare potenziali vittime a mezzo chat, *forum, social network*, tentando di ottenere contatti o incontri con queste ultime.

Il fenomeno "*pedofilia on-line*" è in crescita nell'immensa "giungla" che è la rete *Internet.*

Occorre, dunque, che i genitori inizino una scuola di alfabetizzazione digitale, ed informino i loro figli minori dei rischi che si corrono navigando in rete.

Infatti, Internet costituisce uno strumento formidabile attraverso il quale i propri figli minori possono reperire informazioni, comunicare e dare spazio alla loro creatività.

Pertanto, è consigliabile, dare ai propri figli una appropriata conoscenza e consapevolezza dello strumento digitale che si usa e dell'ambiente digitale in cui si naviga, per evitare che, gli stessi minori, possano incorrere nelle insidie della rete, tipo "adescamenti" *on-line* da parte di sconosciuti.

Quindi, è buona cosa dare giusti ed importanti consigli ai propri figli, quali: 1) non rilevare, mai, a sconosciuti, la propria identità, o i propri indirizzi di casa e della scuola frequentata; 2) non accettare, per nessun motivo, incontri con persone conosciute nelle *chat*, nei *forum o social network*; 3) non divulgare in rete o scambiare proprie foto e video personali e/o di amici, materiale che può essere scaricato e, illecitamente, utilizzato da malintenzionati, quasi sempre pedofili.

E’ bene, inoltre, che i genitori adottino le seguenti precauzioni, a difesa dei propri figli minori, che navigano in Internet: a) controllare la cronologia dei siti visitati dai propri figli minori; b) installare sul personal computer programmi anti-virus da tenere costantemente aggiornati nonché firewall per bloccare connessioni a determinati siti in rete; c) limitare, ai propri figli minori, l’uso di *Internet;* d)predisporre, nelle impostazioni del *browser* del P.C., filtri appositi di accesso a soli determinati siti.

Ciò, nella consapevolezza che i bambini vittime di pedo-pornografia sono tantissimi, per la grande maggioranza bianchi, dai tratti indo-europei; in genere, i bambini asiatici appaiono in immagini dove assumono pose erotiche, più o meno esplicite, come accertato da un progetto elaborato dall’Università di Cork (Islanda), denominato “COPINE” (Combating Paedophile Information Networks in Europe).

Gli stessi consigli, suggerimenti ed accorgimenti devono essere rivolti ai propri figli minori che utilizzano il telefono cellulare e/o gli smartphone, che presentano gli stessi rischi.

Inoltre, è bene sapere, che le immagini pedo-pornografiche vengono diffuse: da un lato, attraverso il canale commerciale, indicizzato su motori di ricerca, oppure accessibile a mezzo di siti pornografici, apparentemente legali e pubblicizzati attraverso lo spamming; dall’altro lato, il canale non commerciale che viene utilizzato per diffondere materiale c.d. “amatoriale”, fatto di immagini prodotte con strumenti “artigianali”, in ambienti “familiari”.

Il Legislatore, per scoraggiare la diffusione del c.d. “turismo sessuale”, ossia la pratica all’estero, in Paesi tolleranti, dello sfruttamento sessuale minorile, è

intervenuto, prima, con la legge 03/08/1998, n. 269 (*"Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù"*).

Successivamente, con la legge 6 febbraio 2006 n. 38, ("*Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo-pornografia anche a mezzo Internet*"), modificando la legge n. 269/98, con la quale ha inasprito le pene a carico di chi si macchia di reati di abuso sessuale.

In particolare, il Legislatore, con la legge n. 38/2006 ha introdotto, le seguenti novità: 1) ampliamento della nozione di pornografia infantile e del suo ambito; 2) l'estensione della protezione accordata al minore fino al compimento del 18^ anno di età; 3) l'interdizione perpetua dall'attività nelle scuole, in ogni ordine e grado, nonché da ogni Ufficio o Servizio in Istituzioni o strutture pubbliche o private, prevalentemente frequentate da minori per le persone condannate per questo tipo di reati e l'esclusione dal patteggiamento per i reati di sfruttamento sessuale; 4) l'individuazione degli elementi costitutivi del reato di sfruttamento sessuale di minori, comuni a tutti gli Stati dell'Unione; 5) iniziative finalizzate ad impedire la diffusione e la commercializzazione dei prodotti pedopornografici via *Internet*: tra queste ha particolare rilievo un sistema di controllo e disattivazione di mezzi di informazione di pagamento, carte di credito ed altro.

La legge n. 38/2006 ha istituito, presso il Ministero dell'Interno, il Centro Nazionale per il monitoraggio della pornografia minorile su Internet con il compito di raccogliere segnalazioni, anche provenienti dall'estero, sull'andamento del fenomeno su rete.

La legge 38/2006 ha ampliato i poteri investigativi al Servizio di Polizia Postale e delle

Comunicazioni, che, su delega dell'A.G. può, d'iniziativa, attivare: a) siti web sotto copertura; b) autorizzare i propri operatori a navigare in Internet sotto copertura, per acquisti e scambi di materiale pedopornografico; c) partecipare, a mezzo di propri poliziotti, operanti sotto copertura, ad iniziative di turismo sessuale.

Il Servizio di Polizia Postale e delle Comunicazioni è una delle specialità della Polizia di Stato, oltre alla Polizia di Frontiera, alla Polizia Stradale, alla Polizia Ferroviaria, e costituisce un Organo Centrale del Ministero dell'Interno Dipartimento della P.S., per garantire la sicurezza e la regolarità dei servizi delle comunicazioni.

La Legge 1 ottobre 2012, n. 172, infine, ha ratificato ed eseguito la Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, disposta a Lanzarote il 25 ottobre 2007, nonchè norme di adeguamento dell'ordinamento interno - Entrata in vigore il 23.10.2012. Tale norma ha introdotto gli articoli 609-bis, 609-quater, 609-quinquies e 609-octies e Art. 414-bis del c.p.. Recentissimo è il Decreto Legislativo del 4 marzo 2014, n. 39 denominato "Attuazione della direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro "2004/68/GAI" e introduce importanti modifiche all'impianto del nostro codice penale in tema di reati concernenti l'abuso sessuale commesso su minori.

8.20) CONTI GIOCO E SCOMMESSE ON-LINE

La crescente diffusione, negli anni, di giochi e scommesse on-line, con l'utilizzo anche di denaro virtuale, ha registrato l'apertura di numerosi siti web dedicati.

Colui che intende accedere a tali servizi, deve registrarsi nell'apposito sito web, e costituire un fondo, mediante versamento di danaro sul sito web attraverso i vari strumenti di pagamento elettronico.

Questi siti-web di gioco on-line, sono gestiti e autorizzati dall'Amministrazione Autonoma Monopoli di Stato (http://www.aams.gov.it), Organo incorporato, in applicazione D.L. 06/07/2012, n. 95, nell'Agenzia delle Dogane e dei Monopoli, che regola il comparto del gioco pubblico in Italia, attraverso una verifica costante dell'operato dei concessionari e una mirata azione di contrasto all'irregolarità.

Ciò premesso, coloro che intendono registrati a questi siti web di scommesse e giochi on-line, devono adottare le dovute precauzioni per evitare che malintenzionati possano carpire i propri dati personali e sensibili.

La registrazione avviene, previa sottoscrizione di un contratto, e contestuale invio dei propri documenti, al gestore del sito *web* di *scommesse e giochi on-line,*

Nello specifico, sarebbe opportuno che i giocatori si registrassero su siti web c.d. "sicuri", utilizzando, preferibilmente, la propria rete domestica o aziendale, protetta da un anti-virus, aggiornato, e/o un "firewall", per bloccare eventuali furti di informazioni.

Pertanto, è sconsigliato servirsi della rete *Internet-point,*

8.21) FURTO DEL TELEFONINO

In caso di furto del proprio telefono cellulare, è opportuno, sporgere, immediatamente, denuncia/querela presso un qualsiasi Commissariato della Polizia di Stato.

La denuncia/querela che deve contenere l'indicazione dei dati identificativi del telefonino, ovvero il codice IMEI (composto di 15 e/o 16 cifre), e il numero dell'utenza mobile, oggetto di furto.

Qualora venga rubato un prodotto Apple (come personale computer, i-phone, i-pad, i-pod), è necessario indicare nella denuncia il numero seriale del prodotto e con quale "ID" è stato registrato. Con tali prodotti è possibile, nel caso di attivazione del servizio i-cloud, tentare di localizzare l'apparecchio oggetto di furto utilizzando un altro dispositivo Apple e attivando l'apposita applicazione (trova il mio i-phone).

Richiedere, inoltre, al proprio gestore telefonico, il duplicato della scheda SIM.

Recentemente anche Google ha lanciato un nuovo servizio gratuito che consente agli utenti Android di localizzare il proprio telefono da remoto in caso di smarrimento o furto, consentendo altresì di localizzare lo smartphone su una mappa, far suonare un allarme e cancellare i dati presenti nella memoria del terminale. Per fare ciò devi preventivamente aver impostato la possibilità di localizzare il cellulare attraverso la rete. Pertanto, portarsi nel menu con l'elenco delle app installate e schiacciare "Impostazioni". Selezionare la voce "protezione" e attivare "Ritrovami" poi "accedi con un account Google" (esempio basato su android versione 4.2.2). Si potrà quindi individuare il cellulare Android collegandoti al sito Internet Gestione Dispositivi Android e nel caso in cui il dispositivo abbia accesso ad Internet e la funzione GPS attiva, lo si potrà visualizzare sulla mappa (E' consigliabile scaricare e installare l'app Gestione dispositivi Android su Google Play).

8.22) MOLESTIE-ATTI PERSECUTORI A MEZZO TELEFONO O RETE INTERNET(CYBER-STALKING)

Per prevenire atti molesti persecutori, sia effettuati da anonimi che persone conosciute realmente o virtualmente, occorre, innanzitutto, adottare le medesime precauzioni elencate quando si è parlato di *chat, forum, mail, social network.*

Se tutto ciò non è stato sufficiente, tanto che il comportamento arriva ad ingenerare nella vittima uno stato permanente di preoccupazione, ansia e terrore, occorre rivolgersi ad un ufficio della Polizia di Stato.

Nel caso in cui la condotta molesta venga messa in opera attraverso l'uso del telefono, indicare date e orari sia dei messaggi (SMS-MMS), che delle telefonate ricevute (anche se si tratta di telefonate anonime o mute) e trascrivendo e/o stampando il contenuto del testo ricevuto.

Occorre precisare se si tratta di un singolo episodio (unico squillo, messaggio, unica chiamata..) o di episodi ricorrenti, potrebbe essere mero errore dell'interlocutore o uno scherzo di pessimo gusto da parte di qualche amico.., il quale però, non lo esime dalle sue responsabilità civili e penali.

Per la rete Internet occorre valutare anche qui in che modo vengono effettuati questi comportamenti intimidatori, persecutori, molestatori.

Se si tratta di mere molestie a mezzo e-mail la soluzione più veloce e indolore è quella di registrare l'indirizzo e-mail del mittente negli spam (vedasi in merito sentenza Cassazione Pen.le Sez. I n. 36779 del 2011"… *sfuggono invece dalla tipicizzazione della condotta come descritta dall'art. 660 c.p. le molestie recate con il mezzo della posta elettronica, perché in tal caso non si verifica nessuna immediata interazione tra il mittente ed il destinatario né veruna intrusione*

diretta del primo nella sfera delle attività del secondo").

Spesso il contenuto delle e-mail degli stalker induce la vittima in uno stato tale da cambiare l'atteggiamento quotidiano, crea timore, ansia. In questo caso occorre stampare le e-mail complete dei dati del mittente e recarsi in un ufficio di Polizia.

Se le molestie, ingiurie, atti diffamatori avvengono su chat, social network, occorre anche qui valutare la gravità della situazione e anche in questo caso copiare la pagina della conversazione e dei messaggi, ove sia evidente il nickname o l'e-mail dell'utente e la stringa URL della pagina web del social network o della chat.

8.23) CYBER BULLISMO

E' un fenomeno che colpisce in genere ragazzi da un'età compresa dai 10 ai 18 anni che per problematiche sociali e caratteriali sfogano i propri atti di bullismo nei confronti dei coetanei non nella vita reale, ma nell'ambiente di Internet, sui social forum, chat, forum etc. Comportamenti che probabilmente nella vita reale non avrebbero il coraggio di fare.

Sono ragazzi dotati di una discreta conoscenza informatica, magari con un'immagine da bravi ragazzi, divulgano a mezzo Internet e telefono foto, immagini di coetanei, i suoi propri pensieri e le proprie difficoltà, li mettono in una situazione di forte imbarazzo, di disagio sociale di discriminazione nel gruppo, utilizzando le proprie credenziali o quelle di altri.

Questi atti di prepotenza possono provocare a chi ne è vittima, uno stato di disagio tale che in taluni casi è culminato con il suicidio della vittima. Le

vittimizzazioni subite in ambito scolastico sono causa di disagi psicologici, sociali e fisici anche a distanza di medio e lungo tempo, influenzando nel caso del cyberbullismo non solo la vita scolastica ma andando oltre nell'ambito personale e sociale della quotidianità del perseguitato. Tra i siti più segnalati per attività di bullismo il più comune è il noto social "http://ask.fm".

Chi è vittima di questi atti non deve vergognarsi di parlarne e confidarsi, né avere timore di eventuali ritorsioni. La comunicazione è importante, lo sfogo con persone adulte (genitori, insegnanti, fratello, sorella, amico/a del cuore, servizi sociali, forze dell'ordine…) è fondamentale a superare queste grosse difficoltà di disagio sociale.

Stesso discorso vale per chi compie questi atti di bullismo, va aiutato a capire che non sono questi comportamenti prevaricatori a renderlo protagonista del branco o del gruppo, ma ne diventa partecipe con ciò che è veramente, sia con le proprie doti e qualità che con i propri difetti. Talvolta, specie tra gli adolescenti, gli scherzi eccessivi si trasformano inconsapevolmente in attività di bullismo vero e proprio.

8.24) VIRUS RANSOMWARE "POLIZIA DI STATO"

La rete Internet, come già più volte detto, è un ambiente fertile e difficilmente tracciabile per chi vuole commettere illeciti. Ultimamente si è diffuso un virus informatico difficile da rimuovere per chi non ha dimestichezza con l'informatica.

Questo virus colpisce principalmente i sistemi operativi Windows ma anche quelli Mac OS X, cambia nome di continuo, ma in gergo comune è conosciuto come virus della Polizia di Stato o Ransomware.

Il cyberware si manifesta, inizialmente, con un avviso a pieno schermo, poi passate 24 ore lo schermo risulta totalmente bianco, con impressi i loghi delle varie forze di Polizia (Carabinieri, Polizia di Stato, Guardia di Finanza, Polizia Postale, Polizia Penitenziaria, FBI..), all'interno del quale è scritto che si è contravventori di una "grave" violazione a seguito di visione di materiale non autorizzato con conseguente blocco del personal computer e per rimuovere il tutto viene chiesto di pagare (in vari modi…) una sanzione (in genere 100 euro).

Non è un vero e proprio virus che carpisce i dati contenuti nel pc, ma è un programma che si attiva quando si accende il pc e blocca ogni processo di avvio.

Ovviamente **non** bisogna pagare nulla perchè **è una truffa**, in quanto, anche se si effettua il pagamento, il PC rimane bloccato. Le Forze dell'Ordine non bloccano il p.c. da remoto e non richiedono pagamenti di sanzioni in rete. Non esiste una vera e propria guida per rimuovere tale virus, in quanto lo stesso si presenta sotto una miriade di varianti, se non si ha dimestichezza si consiglia di rivolgersi a personale tecnico esperto oppure consultare le numerose guide presenti nei vari forum e blog.

8.25) ALCUNI METODI CONSIGLIATI PER LA RIMOZIONE DI TALE VIRUS

a) Metodo consigliato dalla Polizia Postale

Far partire il PC in "Modalità Provvisoria (o Safe Mode)", ossia tenendo premuto il tasto "F8" all'avvio non appena sta per accendersi lo schermo PC; Scegliere la modalità provvisoria con rete e Avviare MSConfig. A questo punto disattivare gli elementi di avvio rundll32 selezionando i programmi da lanciare, poi occorre riavviare ed il pc si dovrebbe avviare normalmente.

In alternativa, una volta avviato il pc in modalità provvisoria bisogna premere

“start” – “Tutti i programmi”, cercare la cartella “Esecuzione automatica”, su XP non ci si arriva in questo modo, ma accedendo a C:/Documents and Settings/NOMEUTENTE/Start menù/Programs/Startup e aprirla;

Visualizzare adesso la lista dei programmi che si avviano automaticamente all’accensione del PC, e tra questi dovrebbe apparire il file “WPBTO.dll”, oppure un file con nome identificativo del tipo “0.< una serie di altri numeri >.exe”;

Eliminare questo file mettendolo nel cestino e poi svuotare anche il cestino;

Riavviare quindi il PC e verificare che tutto funzioni correttamente

b) Utilizzare l’account amministrazione in modalità provvisoria per creare un altro amministratore

Questa soluzione è sicuramente la più rapida ma non indolore, in quanto se non si fa il backup dei dati contenuti si rischia di perderli. Occorre accedere in modalità provvisoria attraverso però l’account amministratore, una volta entrati nella Safe Mode, accedere nel pannello di controllo e andare alla scheda di creazione di un nuovo utente, si trova seguendo il percorso – Account utente><Gestisci account> Crea nuovo account.

Nella schermata occorre cliccare su “Gestisci un altro account” e poi bisogna creare un nuovo account amministratore, occorre quindi salvare immagini, video, musica e anche i file più importanti su un dispositivo esterno. Il problema, adesso, è risolto, infatti una volta riavviato il sistema occorre scegliere il nuovo account amministratore con pieni poteri, il quale ha “ereditato” i programmi del vecchio utente, ma ovviamente non il virus.

Si elimina l’account infetto e con esso il virus.

Come accennato prima il virus cambia di frequente nome, i metodi appena

descritti potrebbero non funzionare, si ricorda che se non si ha dimestichezza in merito è opportuno rivolgersi a personale esperto oppure consultare i vari forum presenti in rete per la risoluzione di questo problema.

8.26) DEEP WEB

Il "*DEEP WEB*" è una parte del Web "*sommersa e invisibile*", è l'insieme delle risorse informative del World Wide Web non segnalate dai normali motori di ricerca.

In essa vengono svolte tantissime attività, da quelle più discutibili e illegali (come la vendita di documenti falsi) ad altre molto più *tranquille*.

Sono, dunque, dei siti "*nascosti*" che non si trovano facendo delle normali ricerche in Google e che possono essere visitati solo sfruttando la rete di anonimizzazione Tor.

Tor può essere definito un sistema di anonimizzazione gratuito che permette di nascondere il proprio indirizzo IP e la propria identità in Rete "*rimbalzando*" la connessione fra vari computer sparsi in tutto il mondo.

8.27) BITCOIN

Il Bitcoin è una moneta elettronica creata nel 2009. Essa è utilizzata per vendere e comprare nel sistema Deep Web.

Il sistema prevede il possesso e il trasferimento anonimo delle monete che sono salvabili su un personal computer sotto forma di "portafoglio virtuale".

Accantonando le complesse nozioni tecniche, ciò che interessa ad un utente Tor sono la reperibilità e l'affidabilità della moneta.

Nel primo caso i siti che vendono e comprano la valuta sono numerosi e

generalmente sicuri, seppur apprestano meccanismi intricati di accesso, appositamente predisposti per i neofiti.

Mentre, per quanto riguarda l'affidabilità della moneta elettronica, la questione è particolarmente delicata, posto che il meccanismo che sta alla base risulta piuttosto complicato, benché l'utilizzo quotidiano di Bitcoin sia piuttosto semplice.

Pertanto, da un lato, chi li utilizza ne sottolinea alcuni vantaggi, quali la facilità con cui effettuare transazioni di somme di danaro, anche da un continente all'altro, in pochi minuti, senza banche, e con costi contenuti.

Diversamente le banche, oltre a rallentare le suddette operazioni di transazione di somme di danaro, applicano costi esosi per il servizio offerto.

Sicché, gli utenti della rete o Tor preferiscono ricorrere all'utilizzo della moneta elettronica (c.d. Bitcoin), che risulta, in ultima analisi, un meccanismo semplice, efficace, veloce per il trasferimento di somme di danaro, oltre a caratterizzarsi per i costi minimi.

Ulteriore vantaggio offerto dalla moneta elettronica (c.d. Bitcoin), è che per il suo utilizzo è sufficiente avere una connessione alla rete Internet, con cui si possono effettuare anche micro-transazioni.

Mentre, dall'altro lato, i pericoli connessi all'utilizzo di detta moneta elettronica (c.d.Bitcoin) sono di molteplici fattori, nella considerazione che si tratta di un meccanismo in fase di sperimentazione e, quindi, costituisce, metaforicamente, "territorio di frontiera".

I pericoli per l'utilizzo della suddetta moneta elettronica, sono di un duplice aspetto: l'uno connesso all'eventualità di un crollo della valuta Bitcoin; l'altro, attinente all'affidabilità dei soggetti, a partire da vari "Exchange", operanti nel settore.

Si consideri, inoltre, che la circolazione della moneta elettronica c.d. Bitcoin in rete, ha favorito il nascere di numerose ed improvvisate imprese individuali, spesso sprovviste delle necessarie risorse economiche per operare nel settore, e sostenere, nel tempo, con continuità,i loro progetti con professionalità.

In questi anni si è detto molto sulla natura di questa nuova forma di pagamento alimentando la convinzione che tale strumento potesse essere utilizzato dalla mafia e dalla criminalità in genere per occultare meglio le loro transazioni finanziarie. In realtà il bitcoin è tracciabile attraverso un sistema creato automaticamente dal software e verificabile dagli organi di polizia paradossalmente in modo più semplice del tracciamento dei flussi di danaro ordinari. Un sistema questo che oggi potrebbe rilevare molti rischi ma dalle grandi potenzialità nelle dinamiche finanziarie globali del prossimo futuro.

9) PER CHI VOLESSE SAPERNE DI PIÙ

”Come tutelarsi nell’era dei social network”. Edito dal Garante della protezione dei dati personali.

La breve guida analizza i principali fenomeni, problemi ed opportunità legate all’uso dei Socia Network, e propone consigli concreti che possano aiutare “nativi digitali” ed utenti alle prime armi, esperti e professionisti. Sul sito del Garante Privacy (www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3140082) potrete trovare maggiori info e scaricare la versione digitale.

Finito di stampare nel Giugno 2014
reproSTAMPA s.r.l. - TIPOLITOGRAFIA
00148 Roma - Via Cesare dal Fabbro, 15
Tel.: 06.6557765 - Fax: 06.65678177
e-mail: info@reprostampa.com