Da inviare in busta chiusa a:

E.BI.PRO.
Viale Pasteur, 65 - 00144 Roma

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI

CONF PROFESSIONI
confederazione italiana libere professioni

CFT sindacati nazionali libere professioni tecniche
Confedertecnica

CGIL FILCAMS

CISL FISASCAT
Federazione Italiana Sindacati Addetti Servizi Commerciali Affini Turismo

UILTuCS

00228815

14

Il rischio informatico per gli studi professionali

Guida informativa

E.BI.PRO.
ENTE BILATERALE NAZIONALE
PER GLI STUDI PROFESSIONALI

Il rischio informatico per gli studi professionali

Guida informativa a cura di Michele Iaselli*

* *Avvocato, Presidente ANDIP (Associazione Nazionale per la Difesa della Privacy), Docente di Informatica giuridica presso la LUISS, vice dirigente Ministero della Difesa.*

Attività di E.BI.PRO.

In continuità con l'impegno assunto con le pubblicazioni dell'ultimo periodo, l'Ente Bilaterale Nazionale per gli Studi Professionali (E.BI.PRO.), in collaborazione con gli altri enti bilaterali di settore (FONDOPROFESSIONI e CADIPROF), prosegue l'attività di informazione su tematiche di alto valore strategico per gli studi professionali.

L'attività di E.BI.PRO. riguarda i seguenti ambiti:

1. **Sostegno al reddito:** Ebipro interviene con un contributo in caso di riduzione dell'orario di lavoro dei dipendenti dovuta a crisi dello studio
2. **Diritto allo studio:** Ebipro prevede forme di sostegno in caso di fruizione dei permessi studio da parte del lavoratore
3. **Salute e sicurezza nei luoghi di lavoro:** Ebipro rimborsa le spese sostenute per la formazione in materia di salute e sicurezza nei luoghi di lavoro.

E.BI.PRO. GESTIONE PROFESSIONISTI

Welfare: Ebipro, sotto la direzione di Confprofessioni e attraverso apposita gestione, prevede una copertura di assistenza per i liberi professionisti.

E.BI.PRO.
ENTE BILATERALE NAZIONALE PER GLI STUDI PROFESSIONALI
Viale Pasteur, 65 - 00144 Roma
Tel. 06.5918786 - Fax 06.94443723
www.ebipro.it – info@ebipro.it

In collaborazione con Wolters Kluwer

E.BI.PRO.
ENTE BILATERALE NAZIONALE PER GLI STUDI PROFESSIONALI
Viale Pasteur, 65 - 00144 Roma
Tel. 06.5918786 - Fax 06.94443723
www.ebipro.it – info@ebipro.it

Fanno parte del sistema di Welfare previsto dal CCNL degli studi professionali anche:

FONDOPROFESSIONI è il Fondo Paritetico Interprofessionale Nazionale per la Formazione Continua dei Lavoratori degli Studi Professionali e delle Aziende Collegate. Istituito nel 2003 con un accordo tra Confprofessioni, Confedertecnica, Cipa e Filcams-Cgil, Fisascat-Cisl e Uiltucs-Uil, Fondoprofessioni nasce con lo scopo di finanziare piani e progetti formativi per consolidare e sviluppare le competenze dei dipendenti degli studi professionali. I piani e i progetti possono essere corsuali, seminariali, individuali e rivolgersi ad una specifica area professionale o trasversali ad essa. L'adesione al fondo è libera e gratuita, il professionista datore di lavoro può scegliere di destinare lo 0,30 % del monte salari, già regolarmente versato all'interno dei contributi Inps, indicando il codice Fpro sulla denuncia mensile di flusso Uniemens.

FONDOPROFESSIONI: diamo risorse alla crescita professionale degli Studi.
www. fondoprofessioni.it - e-mail info@fondoprofessioni.it
tel. 06/54210661 - fax 06/54210664

CADIPROF è la Cassa di Assistenza Sanitaria Integrativa per i lavoratori degli Studi Professionali istituita da Confprofessioni, Confedertecnica, Cipa e Filcams-Cgil, Fisascat-Cisl e Uiltucs-Uil allo scopo di gestire trattamenti di assistenza sanitaria a favore dei dipendenti, secondo quanto previsto dal Ccnl Studi Professionali in vigore. Il Piano Sanitario CADIPROF risponde alle esigenze della popolazione assistita con coperture su misura. La Guida informativa ai servizi, che comprende quelli del "Pacchetto Famiglia", è scaricabile dal sito www.cadiprof.it e illustra le situazioni e le prestazioni coperte dalla Cassa e tutte le procedure da seguire per accedere all'assistenza integrativa, direttamente nelle strutture convenzionate o tramite rimborso.

CADIPROF CASSA DI ASSISTENZA SANITARIA SUPPLEMENTARE PER I DIPENDENTI DEGLI STUDI PROFESSIONALI

CADIPROF: abbiamo cura della salute di chi lavora.
www.cadiprof.it • e-mail info@cadiprof.it • tel. 06/5910526 • fax 06/5918506

Cedola richiesta informazioni

Per approfondimenti e indicazioni più specifiche può rivolgersi a E.BI.PRO.

Visiti il nostro sito internet per saperne di più

E.BI.PRO.
ENTE BILATERALE NAZIONALE PER GLI STUDI PROFESSIONALI

www.ebipro.it

Oppure invii la cedola sottostante in busta chiusa all'indirizzo indicato sul retro.

☐ **Sì, desidero ricevere ulteriori informazioni sull'attività di E.BI.PRO.**

nome e cognome

via

cap

città

e-mail

Ai sensi dell'art. 13 del Codice in materia di dati personali, si informa che il trattamento dei dati personali e sensibili è finalizzato unicamente a fornire informazioni sui nostri servizi. Il trattamento avverrà presso la sede della E.BI.PRO. in Roma con l'utilizzo di procedure informatizzate, nei modi e nei limiti necessari per perseguire le predette finalità. E.BI.PRO. garantisce che il trattamento dei predetti dati avviene secondo modalità idonee a garantirne la sicurezza e la riservatezza e che i dati non verranno utilizzati per finalità difformi da quelle sopra indicate. Per finalità scientifiche e/o statistiche i relativi dati potranno essere rappresentati in forma anonima. I dati potranno essere comunicati solo ad eventuali nostri Collaboratori, Responsabili o Incaricati del trattamento. Il conferimento dei dati è necessario per l'esatta esecuzione degli obblighi contrattuali e di legge e la loro mancata indicazione comporta l'impossibilità di adempiere alle obbligazioni a carico di E.BI.PRO. Agli interessati sono riconosciuti tutti i diritti di cui all'articolo 7 del citato Codice ed in particolare il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento e/o la cancellazione, se incompleti, erronei o raccolti in violazione della legge, nonché di opporsi al loro trattamento per motivi legittimi, rivolgendo le relative richieste per posta al Titolare e Responsabile del trattamento dati per E.BI.PRO. ovvero al suo legale rappresentante pro tempore.

Firma

IL RISCHIO INFORMATICO PER GLI STUDI PROFESSIONALI

Michele Iaselli*

Sommario: 1. Che cosa si intende per cyber risk - 2. L'evoluzione della rete: servizi disponibili on line e rischi connessi - 3. Il concetto di sicurezza informatica - 4. Le misure di sicurezza nel codice della privacy e nel Regolamento europeo sulla protezione dei dati personali - 5. I cybercrimes: nozione e caratteristiche - 6. Gli attacchi provenienti dal Web – 7. Le applicazioni nel settore mobile - 8. Come difendersi dai virus e, in particolare, dalle nuove generazioni di virus (Ransomware) - 9. Ulteriori consigli pratici per evitare truffe informatiche

1. Che cosa si intende per cyber risk

A partire dagli anni novanta, con la nascita e conseguente diffusione di Internet le nuove tecnologie hanno assunto un ruolo sempre più preponderante modificando i rapporti sociali ed individuali, con notevoli ripercussioni in ogni ambito della nostra vita sociale.

Con il passar del tempo, Internet è diventato uno strumento di comunicazione di massa, indispensabile nella vita di tutti i giorni, si pensi alle numerose operazioni che compiamo regolarmente utilizzando il Web, quali inviare una candidatura online tramite un form, condividere dei contenuti sui social, acquistare un viaggio o eseguire un'operazione bancaria, ma rappresenta anche un'opportunità inestimabile per lo sviluppo economico delle imprese, come delle istituzioni scientifiche e pubbliche.

La rivoluzione digitale sta dunque portando molti benefici a società, imprese, studi professionali ma, come spesso accade, bisogna considerare anche il rovescio della medaglia. Difatti, accanto agli innumerevoli benefici, l'uso incontrollato di Internet può comportare una quantità notevole di insidie e problematiche che rientrano nell'ambito di quel fenomeno definito cyber risk "rischio informatico (o ICT)".

In termini metodologici, secondo le linee guida internazionali, storicamente sono classificate 5 grandi famiglie di rischio:

- rischi operativi,
- rischi finanziari,
- rischi strategici,
- rischi organizzativi,
- rischi di pianificazione aziendale e di reporting.

* Avvocato, Presidente ANDIP (Associazione Nazionale per la Difesa della Privacy), Docente di Informatica giuridica presso la LUISS, vice dirigente Ministero della Difesa.

Il cyber risk ha una caratteristica peculiare in quanto può indifferentemente abbracciare ciascuna delle cinque famiglie di rischio citate e considerarsi come una nuova tipologia di macro-rischio determinata dall'evoluzione tecnologica.

Più precisamente, il rischio informatico può essere definito come il rischio di danni economici (rischi diretti) e di reputazione (rischi indiretti) derivanti dall'uso della tecnologia, intendendosi con ciò sia i rischi impliciti nella tecnologia (i cosiddetti rischi di natura endogena) che i rischi derivanti dall'automazione, attraverso l'uso della tecnologia, di processi operativi aziendali (i cosiddetti rischi di natura esogena).

I rischi di natura endogena sono:

- *naturali*: incendi, calamità naturali, inondazioni, terremoti;
- *finanziari*: variazione dei prezzi e dei costi, inflazione;
- *strategici*: concorrenza, progressi scientifici, innovazioni tecnologiche;
- *errori umani*: modifica e cancellazione dei dati, manomissione volontaria dei dati.

I rischi di natura esogena, o di natura operativa sono i rischi connessi alle strutture informatiche che compongono i sistemi. Essi sono:

- danneggiamento di hardware e software;
- errori nell'esecuzione delle operazioni nei sistemi;
- malfunzionamento dei sistemi;
- programmi indesiderati.

Tali rischi possono verificarsi a causa dei cosiddetti programmi "virus" destinati ad alterare od impedire il funzionamento dei sistemi informatici. Ma vi sono anche le truffe informatiche, la pedo-pornografia, il cyberbullismo, i ricatti a sfondo sessuale derivanti da video chat on line e solo una piena consapevolezza del concetto di sicurezza informatica può davvero metterci al riparo da sgradevoli sorprese.

Ogni giorno vengono compiuti migliaia di attacchi informatici attraverso le tecniche più varie e termini come malware, ransomware, trojan horse, account cracking, phishing, 0-dayvulnerability sono diventati parte del vocabolario anche per i non esperti.

J. Edgar Hoover, capo dell'FBI (Federal Bureau of Investigation) moltissimi anni fa affermava: "*L'unico computer a prova di hacker è quello spento, non collegato ad Internet e chiuso a chiave in una cassaforte*". Appena viene riacceso diventa potenzialmente vulnerabile e può essere attaccato, ad esempio durante l'installazione di eventuali aggiornamenti al sistema operativo.

Per evitare attacchi informatici, o almeno per limitarne le conseguenze, è necessario adottare delle contromisure; i calcolatori e le reti di telecomunicazione necessitano di protezione anche se come in qualsiasi ambiente la sicurezza assoluta non è concretamente realizzabile.

Il modo per proteggersi è imparare a riconoscere le origini del rischio.

Gli strumenti di difesa informatica sono molteplici, si pensi antivirus, antispyware, blocco popup, firewall ecc., ma tuttavia non sempre si rivelano efficienti, in quanto esistono codici malevoli in grado di aggirare facilmente le difese, anche con l'inconsapevole complicità degli stessi utenti.

Di recente si sta assistendo alla nascita di una nuova modalità di prevenzione del rischio informatico: il Trusted Computing.

L'espressione inglese Trusted Computing (TC, letteralmente informatica fidata o calcolo fidato) si riferisce ad una tecnologia nascente, con l'obiettivo dichiarato di rendere dispositivi come computer o telefoni cellulari più sicuri mediante l'uso di opportuni hardware o software.

Il TC si basa sull'uso della crittografia. Dunque l'obiettivo del TC non è quello di introdurre nuovi strumenti software per fronteggiare i rischi ed attacchi connessi a sistemi informatici ed a reti di telecomunicazioni, ma bensì di costruire sistemi hardware o software non abilitati a determinate funzioni in grado di comprometterne la sicurezza, nonché il controllo attraverso Internet, del rispetto delle limitazioni di funzionalità da parte degli utenti dei sistemi.

Un altro aspetto di notevole importanza del rischio informatico e di interesse per gli studi professionali su cui dobbiamo soffermare la nostra attenzione è il risk management.

Il risk management (gestione del rischio) è quel processo attraverso il quale si misura o si stima il rischio e successivamente si sviluppano le strategie per fronteggiarlo.

La gestione del rischio, così come descritto nella Convenzione Interbancaria per i problemi dell'Automazione (CIPA) nel rapporto sul rischio informatico si articola in diverse fasi:

• identificazione del rischio;
• individuazione delle minacce;
• individuazione dei danni che posso derivare dal concretizzarsi delle minacce e la loro valutazione;
• identificazione delle possibili contromisure per contrastare le minacce arrecate alle risorse informatiche.

Diverse sono le modalità di gestione del rischio. A seconda del livello di rischio che un soggetto sia esso un'azienda, persona o ente ritiene accettabile si distinguono:

• Evitare: si modificano i processi produttivi, modalità di gestione ed amministrazione con lo scopo di eliminare il rischio.

• Trasferire il rischio ad un altro soggetto: il trasferimento del rischio avviene nei confronti di assicurazioni, partner e si tratta principalmente di rischi economici perché più facilmente quantificabili.

• Mitigare: consiste nel ridurre, attraverso processi di controllo e verifica, la probabilità del verificarsi del rischio o nel limitarne la gravità delle conseguenze nel caso in cui si verifichino.

• Accettare: ossia assumersi il rischio ed i relativi costi.

Da alcuni anni l'interesse degli operatori economici sul cyber risk è cresciuto notevolmente. Questa crescita è stata tale da suscitare l'interesse delle compagnie di assicurazione su questa tipologia di rischio.

Negli Stati Uniti le polizze assicurative esistono da più di 15 anni, mentre invece in Italia sono state introdotte solo da pochi anni.

2. L'evoluzione della rete: servizi disponibili on line e rischi connessi

Molto spesso sentiamo parlare di Web 1.0, 2.0, 3.0 senza conoscerne il reale significato e le differenze tra essi. Ma cosa si intende per Web?

Il Web è uno spazio elettronico e digitale destinato alla pubblicazione di contenuti multimediali (testi, immagini, audio, video, ipertesti, ipermedia ecc.), nonché uno strumento per implementare particolari servizi come ad esempio il download di software (programmi, dati, applicazioni, videogiochi ecc.).

Tale spazio elettronico e tali servizi sono resi disponibili attraverso particolari computer collegati in rete chiamati server Web. Si è soliti ricondurre la nascita del Web (il World Wide Web letteralmente "rete di grandezza mondiale") al 6 agosto 1991, giorno in cui Tim Berners-Lee, informatico britannico, pubblicò il primo sito Web dando così vita al fenomeno "WWW" (detto anche "della tripla W").

L'evoluzione del Web si articola in diverse fasi:

Il Web 1.0 (il suffisso 1.0 fu aggiunto successivamente per differenziarlo dall' evoluzioni di Web successive) era caratterizzato dalla presenza di siti Web statici e non interattivi, erano formati da pagine ricche di ipertesti, contenenti collegamenti ad altre pagine.

Il Web 2.0 viene inteso come evoluzione della rete e dei siti internet, caratterizzati da una maggiore interattività che pone l'utente al centro della rete. Internet non è più una semplice "rete di reti", né un agglomerato di siti Web isolati e indipendenti tra loro, bensì la "summa" delle capacità tecnologiche raggiunte dall'uomo nell'ambito della diffusione dell'informazione e della condivisione del sapere.

In altri termini il Web 2.0 è l'insieme di tutte quelle applicazioni online che permettono un elevato livello di interazione tra il sito Web e l'utente come i blog, i forum, le chat, i wiki, le piattaforme di condivisione di media come Youtube, social network, ecc.

Il termine Web 3.0 è stato coniato da Etic Schmidts (ceo di Google) nel 2007. La linea di sviluppo principale che caratterizza il Web 3.0 è il concetto di Web semantico (semantic Web). Il termine Web semantico fa riferimento all'inserimento nel Web di informazioni comprensibili da parte del calcolatore.

Il Web attuale corrisponde solo in piccola misura all'idea del Web semantico che nasce dalla necessità di facilitare lo scambio di informazioni non solo tra gli uomini, che si realizza con il Web 2.0, ma anche tra le macchine.

In sintesi, possiamo dire che il Web 3.0 è caratterizzato da contenuti comprensibili dal computer, dal collegamento dei dati grazie a criteri di classificazione comuni e, infine, dall'Internet of Things (IoT), neologismo riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti dove l'oggetto ha un ruolo attivo, dinamico, interagisce con il mondo circostante in modo intelligente, grazie a una serie di "sensori" e "attuatori" e tramite un collegamento alla Rete.

Oggi già sono immessi in commercio elettrodomestici programmabili a distanza (domotica) o che comunque grazie al collegamento alla Rete sono in grado di fornire ulteriori informazioni al consumatore (possibili guasti, consumi di elettricità, ecc.).

Sin dall'inizio la Rete ha messo a disposizione dei propri utenti tantissimi servizi, ricordiamo le mailing-list, i newsgroup, i personal Web site per poi passare ai più moderni wiki, blog, social network (facebook, twitter, linkedin, myspace, youtube, ecc.). Spesso questi servizi sono gratuiti, ma i gestori di queste piattaforme sociali in cambio ci chiedono i nostri dati personali al fine di poter tracciare le nostre identità digitali. In questo modo è possibile profilarci e condurre efficaci politiche di marketing a vantaggio di aziende talvolta prive di scrupoli.

Bisogna stare attenti alle attività delle aziende che gestiscono i social network, in quanto generalmente si finanziano vendendo pubblicità mirate. Il valore di queste imprese è strettamente legato anche alla loro capacità di analizzare in dettaglio il profilo, le abitudini e gli interessi dei propri utenti, per poi rivendere le informazioni a chi ne ha bisogno.

I social network (Facebook, MySpace e altri) sono "piazze virtuali", cioè dei luoghi in cui via Internet ci si ritrova portando con sé e condividendo con altri fotografie, filmati, pensieri, indirizzi di amici e tanto altro.

I social network sono lo strumento di condivisione per eccellenza e rappresentano straordinarie forme di comunicazione, anche se comportano dei rischi per la sfera personale degli individui coinvolti. Sono strumenti che danno l'impressione di uno spazio personale, o di piccola comunità. Si tratta però di un falso senso di intimità che può spingere gli utenti a esporre troppo la propria vita privata, a rivelare informazioni strettamente personali, provocando "effetti collaterali", anche a distanza di anni, che non devono essere sottovalutati.

Non bisogna mai dimenticare che le nozioni di *digital footprint*, identità e profilazione degli utenti in internet, sono concetti tra loro strettamente collegati.

Il termine *digital footprint*, viene comunemente utilizzato per indicare le tracce di dati che vengono disperse nella rete a seguito di determinate interazioni avvenute all'interno dell'ambiente digitale, questi dati contengono

usualmente informazioni riguardanti le diverse interazioni che un soggetto può eseguire in un contesto digitale. Questi dati ed informazioni possono concorrere nel formare anche una identità digitale.

A tal fine è possibile individuare almeno due tipi di informazioni che possono essere reperite on-line e riguardanti un soggetto determinato, un primo tipo, che potremmo definire di *informazioni primarie* e riguardanti i caratteri personalissimi dell'individuo, ed altri tipi di *informazioni secondarie*, riguardanti le abitudini sociali ed i gusti commerciali dell'utente interessato, questi due tipi di informazioni, elaborate tra loro, formano il cd. profilo-utente.

Da queste brevi premesse, si pongono alla nostra attenzione una serie di questioni, occorre anzitutto domandarsi quali siano gli interessi che sottostanno ad una operazione di profilazione e in seconda analisi quali tutele sono esperibili in tali situazioni.

Come noto, la maggior parte dei moderni dispositivi di comunicazione, al momento del loro utilizzo attraverso il collegamento ad internet, frammentano e disperdono delle tracce che provano l'utilizzo del dispositivo e la contestuale presenza dell'utente in rete. Nella pratica il problema della profilazione e della dispersione dei dati personali, si manifesta in modo particolare nei momenti della navigazione in internet mediante browser (si pensi ai cookies) e nell'utilizzo delle più comuni piattaforme di social networking come strumenti relazionali e di comunicazione.

A tal fine vengono sempre più utilizzate anche tecniche di reperimento di informazioni utili al ciclo di intelligence tramite il monitoraggio e l'analisi dei contenuti scambiati attraverso i Social Media come la SOCial Media INTelligence (SOCMINT).

L'obiettivo principale della profilazione è la pubblicità comportamentale, che pensata e cresciuta nel mondo delle comunicazioni informatiche, prevede il tracciamento delle informazioni rilasciate dagli utenti durante la navigazione in internet, al fine di creare segmenti pubblicitari *ad personam*, modellati sugli interessi dell'utente considerato. Tale attività di per sé non è illecita o vietata, ma con il crescente bisogno di proteggere le identità digitali e i dati sensibili degli utenti, negli ultimi anni l'Unione europea si è mossa in maniera molto decisa verso la creazione di direttive e linee guida contenenti discipline di regolamentazione nelle comunicazioni elettroniche e di protezione dei dati nonché delle informazioni riguardanti gli utenti di internet, per dare ai naviganti strumenti attraverso i quali poter essere sempre al corrente dell'eventuale monitoraggio che può avvenire sulle loro tracce digitali. Il recente Regolamento europeo in realtà ha un occhio particolare per tali attività che vengono considerate degne della massima attenzione.

In effetti il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e

rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Difatti, nell'attuale era tecnologica, come si è visto, le caratteristiche personali di un individuo possono essere tranquillamente scisse e fatte confluire in diverse banche dati, ciascuna di esse contraddistinta da una specifica finalità. Su tale presupposto può essere facilmente ricostruita la c.d. persona elettronica (v. identità digitale) attraverso le tante tracce che lascia negli elaboratori che annotano e raccolgono informazioni sul suo conto.

La forma di tutela più efficace è comunque sempre l'autotutela, cioè la gestione attenta dei propri dati personali. Difatti, i contenuti creati dagli utenti e resi pubblici attraverso il mezzo telematico, costituiscono un potenziale veicolo di violazioni degli interessi di terzi e in questo senso una minaccia per diritti quali l'immagine, l'onore e la reputazione, nonché la riservatezza. Come messo in risalto da alcuni interpreti, la rete, che per sua natura tende a connettere individui, formazioni sociali e istituzioni di ogni genere, pone questioni "inquietanti" in quanto risolvibili solo con nuovi approcci, soluzioni mai adottate prima e in taluni casi non ancora individuate.

Quando si inseriscono i propri dati personali su un sito di social network, si perde il controllo degli stessi. I dati possono essere registrati da tutti i propri contatti e dai componenti dei gruppi cui si è aderito, rielaborati, diffusi, anche a distanza di anni.

A volte, accettando di entrare in un social network, si concede all'impresa, che gestisce il servizio, la licenza di usare senza limiti di tempo il materiale che viene pubblicato on-line e quindi le proprie foto, chat, scritti, pensieri.

Questo aspetto deve far riflettere anche lo studio professionale che, laddove dovesse decidere di sfruttare le potenzialità dei social network per scopi promozionali o di marketing, dovrà porre la massima attenzione alla gestione dei dati personali dei potenziali clienti.

Inoltre, se si decide di uscire da un sito di social network spesso si prevede solo la possibilità di "disattivare" il proprio profilo, non di "cancellarlo". I dati, i materiali pubblicati on-line, potrebbero essere comunque conservati nei server, negli archivi informatici dell'azienda che offre il servizio. È necessario, quindi, leggere bene cosa prevedono le condizioni d'uso e le garanzie di privacy offerte nel contratto ed accettate dagli utenti al momento dell'iscrizione.

D'altro canto, la maggior parte dei siti di social network ha sede all'estero e così i loro server. In caso, quindi, di disputa legale o di problemi

insorti per violazione della privacy, non sempre si è tutelati dalle leggi italiane ed europee.

3. Il concetto di sicurezza informatica

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software ed i dati dagli accessi non autorizzati (intenzionali o meno), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

Si include, quindi, la sicurezza del cuore del sistema informativo, cioè il centro elettronico dell'elaboratore stesso, dei programmi, dei dati e degli archivi. Questi problemi di sicurezza sono stati presenti sin dall'inizio della storia dell'informatica, ma hanno assunto dimensione e complessità crescenti in relazione alla diffusione e agli sviluppi tecnici più recenti dell'elaborazione dati; in particolare per quanto riguarda i data base, la trasmissione dati e l'elaborazione a distanza (informatica distribuita). Non è, ad esempio, da sottovalutare il rischio cui può andare incontro il trasferimento elettronico dei fondi tra banche oppure il trasferimento da uno Stato all'altro di intere basi di dati reso possibile dai moderni sistemi di trasmissione telematica.

Riguardo l'aspetto "sicurezza" connesso alla rete telematica, essa può essere considerata una disciplina mediante la quale ogni organizzazione, che possiede un insieme di beni, cerca di proteggerne il valore adottando misure che contrastino il verificarsi di eventi accidentali o intenzionali che possano produrre un danneggiamento parziale o totale dei beni stessi o una violazione dei diritti ad essi associati. Un bene può essere un'informazione, un servizio, una risorsa hardware o software e può avere diversi modi possibili di interazione con un soggetto (persona o processo). Se, ad esempio, il bene è un'informazione, ha senso considerare la lettura e la scrittura (intesa anche come modifica e cancellazione); se invece il bene è un servizio, l'interazione consiste nella fruizione delle funzioni offerte dal servizio stesso.

Naturalmente è chiaro che in un sistema complesso nel quale interagiscono più soggetti, la sicurezza potrà essere garantita solo se:

1. le azioni lecite che ciascun soggetto può eseguire interagendo con i beni cui può accedere tramite la rete, saranno correttamente individuate e definite;

2. il sistema verrà definito in tutti i suoi aspetti (tecnici, procedurali, organizzativi, ecc.), in modo tale che le possibili azioni illecite, eventualmente attuate sia da parte di estranei che di utenti della rete, siano contrastate con un'efficacia tanto maggiore quanto più elevati sono i danni conseguenti all'azione illecita considerata.

Il soddisfacimento delle due condizioni richiede lo sviluppo di una politica di sicurezza nell'ambito della quale:

- venga scelto, con il criterio del minimo danno per un ente, l'insieme delle autorizzazioni che specificano i modi di interazione leciti di ogni soggetto con i beni cui si può accedere tramite la rete;

- vengano selezionate, applicando al sistema una metodologia di analisi e gestione dei rischi, le contromisure di tipo tecnico, logico (dette anche funzioni di sicurezza), fisico, procedurale e sul personale che permettano di ridurre a livelli accettabili il rischio residuo globale.

Il primo passo per lo sviluppo di una politica di sicurezza per uno studio professionale è la definizione delle autorizzazioni che disciplinano l'uso dei beni.

Tale definizione può avvenire attraverso le seguenti fasi:

1. identificazione dei beni;
2. quantificazione del valore dei beni;
3. classificazione dei soggetti dal punto di vista dell'affidabilità;
4. applicazione di predefinite regole di autorizzazione.

L'organizzazione, per decidere quali autorizzazioni concedere ad un prefissato soggetto, dovrà valutare, per ogni bene e per ogni tipo di interazione con esso, quali eventuali danni possano derivare dalla concessione o dalla negazione della corrispondente autorizzazione. L'entità di tali danni potrebbe essere allora utilizzata per definire i valori del bene relativi al particolare tipo di interazione da parte del soggetto considerato.

L'insieme delle autorizzazioni può essere anche definito come l'insieme degli obiettivi di sicurezza per il sistema funzionante in accordo con la politica di sicurezza stessa. Gli obiettivi di sicurezza vengono generalmente definiti come requisiti di riservatezza (prevenzione dell'utilizzo indebito di informazioni riservate), integrità (prevenzione dell'alterazione o manipolazione indebita di informazioni) e disponibilità (prevenzione dell'occultamento o dell'impossibilità di accesso a dati o risorse necessarie alla conduzione dell'attività) espressi con riferimento ai beni da proteggere.

Ovviamente, un sistema ideale dal punto di vista della sicurezza non esiste. Un sistema reale può però essere dotato di contromisure che rendano molto difficile il verificarsi di eventi non compatibili con il rispetto delle autorizzazioni.

La sicurezza può essere garantita in diversi modi:

- *tramite mezzi di accesso fisici*. Questi sono consegnati all'utente legittimo ed egli esclusivamente ne viene in possesso e ne è responsabile. Tali mezzi sono costituiti da documenti di riconoscimento tradizionali, da chiavi meccaniche di varia forma e complessità, da chiavi elettroniche (c.d. tesserini magnetici di riconoscimento, carte di credito). Ciascuno di questi strumenti può essere considerato come una forma di legittimazione e di accesso controllato. Detti mezzi non sono, in genere, usati da soli, salvo che in ambienti poco attenti ai problemi della sicurezza. Infatti contraffazione e duplicazione sono abbastanza praticabili con tecnologie di medio livello e, quel

che è più pericoloso, i predetti mezzi di identificazione possono essere sottratti o ceduti a soggetti non autorizzati. Pertanto, il livello di sicurezza viene accresciuto, in alcuni casi, con la combinazione di tali strumenti con quelli di seguito indicati;

- *tramite mezzi di accesso memorizzati dall'utente legittimo*. Essi consistono in una sequenza di elementi (numerici, alfabetici o simbolici) che vengono forniti segretamente e memorizzati dall'utente legittimo e da questo forniti al sistema al momento in cui si vuole accedere allo stesso.

Tra i principali mezzi di accesso rientranti in questa categoria si ricordano:

1. il P.I.N. (Personal Identification Number): si tratta di un numero di identificazione personale che viene attribuito in maniera segreta esclusivamente all'utente legittimo. Tale numero va scritto su un'apposita tastiera numerica al momento in cui si accede al computer;

2. la Password, ossia la c.d. "parola chiave": si tratta di una parola, o di una sequenza di lettere e numeri, anche complessa, memorizzata dall'utente legittimo e che deve essere scritta, in genere su una tastiera. Detta combinazione alfanumerica va opportunamente scritta con rapidità per evitare che malintenzionati riescano a seguire la sequenza dei tasti premuti e a ricavare così, la parola chiave;

3. la combinazione numerica-logica variabile: in alcuni casi la parola chiave non è fissa, ma varia dinamicamente con riferimento ad una parte di elementi fissi ed altri variabili. Per esempio, una combinazione dinamica può essere rappresentata dalla sommatoria di un certo numero conosciuto dall'utente, addizionato, sottratto, diviso o moltiplicato ad un altro numero che potrebbe variare con riferimento al giorno della settimana, alla data completa, ovvero ad un dato variabile.

Tramite mezzi di accesso che confrontano caratteristiche fisiche dell'utente con quelle memorizzate dal sistema (i cd. sistemi biometrici).

Si tratta della ricerca più avanzata in tema di sicurezza degli accessi informatici.

Tra i sistemi biometrici si ricordano:

1. le impronte digitali e le impronte palmari;

2. il riconoscimento della voce (difettoso in caso di malattie da raffreddamento);

3. il reticolo venoso della retina dell'occhio;

4. il controllo dinamico della firma (firma grafometrica).

4. Le misure di sicurezza nel codice della privacy e nel Regolamento europeo sulla protezione dei dati personali

Il Codice per la protezione dei dati personali prevede all'art. 33 le c.d. misure minime di sicurezza che consistono in tutta una serie di misure da

adottare per garantire la sicurezza minima al trattamento dei dati e che naturalmente devono essere implementate anche dallo studio professionale.

La disposizione in esame prende spunto dall'art. 15 comma 2 della legge n. 675/96, sancendo l'obbligo per i titolari del trattamento di adottare le misure minime di sicurezza previste dalla normativa. Rispetto al precedente art. 15, la disposizione in argomento individua con precisione il titolare del trattamento come destinatario fondamentale della disciplina della sicurezza. In effetti il responsabile è solo una figura eventuale, che ripete i propri poteri dal titolare del trattamento, anche se la nomina è effettuata tra soggetti che forniscano idonea garanzia del pieno rispetto delle disposizioni, ivi compreso il profilo relativo alla sicurezza.

Le misure minime sono elencate nell'art. 34 (per i trattamenti a mezzo elaboratore elettronico) e 35 (per i trattamenti senza elaboratore elettronico) del Codice.

L'art. 34 del Codice non trova specifici precedenti nella pregressa normativa sulla privacy. Esso disciplina ed elenca principalmente le misure minime di sicurezza da adottare nel caso di trattamenti di dati personali effettuati con strumenti elettronici, demandando la determinazione delle modalità di applicazione alle disposizioni contenute nel Disciplinare tecnico allegato al codice (allegato B).

Per i trattamenti effettuati con strumenti elettronici, il nuovo codice della privacy richiede che:

- il sistema disponga di strumenti di autenticazione degli utenti. Nel D.P.R. n. 318/99, come si ricorderà, si parlava solo di password, mentre non erano riconosciute valide funzioni di autenticazione più robuste, come ad esempio, la firma digitale o le impronte digitali;
- il titolare adotti appropriate procedure, con la caratteristica della periodicità, per mantenere aggiornate le utenze ed i relativi profili di accesso sia per gli utenti normali, sia per quelli che sono addetti alla gestione o manutenzione dei sistemi. C'è da osservare, sul punto, che i precedenti ruoli di amministratore di sistema (oggetto di specifico provvedimento del Garante) e custode delle password non sono citati dal d.lgs. n. 196/2003, ma rientrano nella più generale categoria degli addetti alla gestione;
- sia definito un sistema di autorizzazione per abilitare gli utenti all'accesso ai dati e/o ai trattamenti;
- gli strumenti elettronici e i dati siano protetti da accessi non autorizzati da parte di utenti, programmi informatici e da trattamenti illeciti (antivirus, firewall, ecc.);
- il titolare adotti appropriate procedure per il backup dei dati, il loro recupero, nonché il ripristino della disponibilità dei sistemi e dei dati;
- l'obbligo di adottare tecniche di cifratura per i trattamenti atti a rivelare lo stato di salute o la vita sessuale rilevati da organismi sanitari.

Come è noto l'obbligo della redazione del Documento programmatico sulla sicurezza è stato eliminato dall'art. 45 dell'ormai celeberrimo "Decreto Semplificazioni" ovvero il D.L. 9 febbraio 2012, n. 5, così come convertito con modificazioni dalla Legge 4 aprile 2012, n. 35, denominato "Disposizioni urgenti in materia di semplificazione e di sviluppo".

Ma oltre alle misure minime di sicurezza esistono anche le misure idonee di sicurezza menzionate nell'art. 31 del Codice per la protezione dei dati personali, che contiene un obbligo di sicurezza nei confronti sia dei titolari del trattamento dei dati in senso stretto, sia nei confronti di chiunque effettui un trattamento dei dati anche per scopi personali secondo quanto previsto dall'art. 5 comma 3.

La norma in esame non precisa quali misure specifiche adottare, si limita solamente a prescrivere l'obbligo, lasciando al soggetto obbligato la scelta in ordine a quali misure di sicurezza implementare.

Quest'obbligo consiste nel garantire che il trattamento dei dati personali sia sicuro in modo da "*ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Il trattamento inoltre deve assicurare che i dati siano custoditi e utilizzati in relazione alle conoscenze acquisite in base al progresso tecnico*".

In dottrina è stato giustamente affermato che il richiamo del progresso tecnico implica l'applicazione di una tecnologia affidabile, che sia stata introdotta in scala nel mercato e non una tecnologia sperimentale.

Si ritiene che il riferimento al progresso tecnico sia un aspetto cruciale, che permette di cogliere la distinzione tra le misure minime di sicurezza volte a garantire un livello minimo di sicurezza, il quale non richiede un controllo dell'efficacia delle misure implementate se non minimale, e le misure idonee, che invece richiedono un controllo dell'efficacia delle stesse.

Non poteva, ovviamente, mancare anche nel Regolamento europeo n. 2016/679 sulla protezione dei dati personali (che diventerà obbligatorio a decorrere dal 25 maggio 2018) un chiaro riferimento alle misure di sicurezza che già vengono menzionate nell'art. 22, quando si chiarisce che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento (principio di accountability). Mentre, più nello specifico, l'art. 32 del Regolamento ne parla a proposito della sicurezza del trattamento.

Tenuto conto, quindi, dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile

del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

5. I cybercrimes: nozione e caratteristiche

Dare una definizione di crimine informatico meglio noto come cybercrime, non è semplice poiché tale termine include al proprio interno diverse condotte illecite, di varia natura, aventi come denominatore comune l'utilizzo di un computer o di un dispositivo informatico.

In genere, per crimine informatico si intende un qualunque comportamento criminoso, nel quale il computer è coinvolto come mezzo o come oggetto dell'azione delittuosa, ma in tale categoria rientrano anche quegli illeciti in cui il computer si interpone tra l'autore del crimine e la vittima o, comunque, rappresenta lo strumento principale per compiere una determinata azione criminosa.

È possibile, inoltre, distinguere tra:

reati eventualmente informatici	reati in cui le tecnologie informatiche hanno solo ampliato le modalità di realizzazione di un reato già esistente, un esempio può essere rappresentato dal furto o dall'appropriazione indebita di fondi realizzati utilizzando le tecnologie informatiche
reati necessariamente informatici	hanno comportato la nascita di figure criminose completamente nuove, un esempio è dato dal delitto di accesso abusivo ad un sistema informatico o telematico (art 615-*ter* c.p.)
computer fraud	comprendono tutti i comportamenti manipolativi con scopi fraudolenti
computer abused	integrano tutte le condotte che prevedono degli usi impropri delle tecnologie al fine di ottenere vantaggi

Il trattato del Consiglio d'Europa sulla criminalità informatica definisce il "cybercrime" come quei "reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici", si pensi ad esempio: all'accesso illegale", alle "intercettazioni illegali", ecc.

Si suole distinguere i crimini informatici in tre categorie:

- *attacchi criminali propriamente intesi* che hanno come obiettivo comune la violazione di un sistema informatico al fine di ottenere un guadagno economico. Tra questi rientrano la frode informatica, che si ha quando chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico e telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno. (art. 640-*ter* c.p.);

- *attacchi non propriamente criminali* che sono gli attacchi a scopo pubblicitario, ossia quelli che mediante la pubblica violazione di un sistema informatico, mirano a creare disagio al fine di richiamare l'attenzione della stampa e, quindi, suscitare un'eco mediatica;

- *attacchi basati su sistemi legali* che si fondano sulla debolezza del sistema giudiziario, il loro obiettivo è quello di screditare dal punto di vista legale alcune apparenti sicurezze informatiche.

Secondo un'attenta ricerca i cybercrimini si differenziano dai crimini tradizionali in quanto:

a) sono tecnicamente più semplici da commettere in quanto non richiedono particolari conoscenze informatiche;

b) non richiedono un investimento criminale iniziale ingente, considerando il profitto che da essi può derivare;

c) possono essere commessi in ogni parte del mondo, in quanto non è richiesta la presenza fisica al momento della consumazione del fatto;

d) su di essi non sempre v'è chiarezza ed uniformità normativa a livello europeo ed internazionale.

6. Gli attacchi provenienti dal Web

Quando si parla di attacchi provenienti dal Web non si può fare a meno di pensare ai virus, ma vedremo che non sono gli unici pericoli e tra l'altro non sono tutti uguali.

Un *virus informatico* è composto da un insieme di istruzioni da pochi byte ad alcuni kilobyte (per rendere più difficile da individuare e facile da copiare), tende ad eseguire soltanto poche operazioni ed impiega il minor numero di risorse, in modo da rendersi il più possibile invisibile.

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:

1. ricercare i file adatti ad essere infettati controllando che non contengano già una copia, per evitare una ripetuta infezione dello stesso file;

2. copiare il codice virale all'interno di ogni file selezionato perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

A seconda del tipo di danni causati, i virus si distinguono in:

- *innocui*: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer;
- *non dannosi*: se comportano una diminuzione dello spazio libero sul disco mostrando grafici, suoni o altri effetti multimediali;
- *dannosi*: possono provocare, ad esempio, cancellazione di alcune parti dei file;
- *molto dannosi*: causano danni difficilmente recuperabili come la cancellazione d'informazioni fondamentali per il sistema (formattazione di porzioni del disco).

Ma quando sentiamo parlare di virus, in genere ricomprendiamo malware, trojan horse, worm mettendoli tutto sullo stesso piano sia per genesi che per effetti, invece, è necessario fare delle precisazioni in quanto esistono delle sostanziali differenze tra queste diverse tipologie di virus.

In primo luogo c'è da precisare che sia i virus, sia i trojan horse che i worm rientrano nella categoria più generale dei malware.

Il termine malware deriva dalla contrazione di due termini inglesi, rispettivamente "MALicious" e "softWARE", e viene utilizzato per indicare tutti quei programmi realizzati per danneggiare le macchine che li eseguono, da qui il nome di software malevolo. I programmi malware se riescono ad entrare in un computer possono creare dei veri e propri danni impedendone il corretto funzionamento, oppure possono spiare tutto quello che scriviamo, sottrarre dati sensibili, come ad esempio i numeri della carta di credito, per trasmetterli poi ad altri malintenzionati.

Gli obiettivi alla base di tutti i programmi rientranti in questa categoria sono:

- *installarsi* sul dispositivo e *nascondersi* all'utente, in modo da poter sopravvivere il più a lungo possibile;
- *propagarsi* il più possibile aumentando in questo modo il numero di successi.

Tuttavia ogni tipologia di codice virale pur usando strumenti, tecnologie e tattiche diverse, possiede un unico modello strutturale, basato su quattro fasi:

1. *Infezione*: il malware si introduce all'interno del sistema, superando eventuali barriere di sicurezza, installandosi al suo interno. L'introduzione avviene mediante l'esecuzione di un file contenente, in modo diretto o indiretto, il codice virale. Tale introduzione che può avvenire mediante il trasferimento fisico, modalità, molto diffusa in passato, ma ancora oggi frequente, prevede l'uso di un supporto di memorizzazione (come floppy disk,

CD o unità USB) da parte dell'utente malevolo o, inconsapevolmente, della vittima stessa e prevede un accesso fisico al PC.

Ma il malware può anche essere allegato a messaggi di posta elettronica (spam): l'utente viene così invitato ad aprire l'allegato, che può essere un file eseguibile o anche un documento elettronico. "Melissa" è stato il primo malware che ha usato questo canale di diffusione ed ha infettato in breve tempo oltre ottantamila sistemi, causando danni a livello mondiale.

Infine l'introduzione può avvenire anche via Web (e ad oggi questo è il canale di diffusione più frequente) trasmettendo il codice malevolo attraverso un download da una pagina Web.

2. *Quiescenza*: una volta introdotto nel sistema, il malware resta residente in memoria, in attesa che l'utente compiendo una determinata azione lo avvii. Per auto proteggersi da eventuali rilevamenti da parte dell'utente o da un software di sicurezza, gli attaccanti assegnano al processo malevolo il nome di un programma presente nel proprio computer ad esempio "internetexplorer" in modo da rendere difficile l'individuazione da parte dell'utente.

3. *Replicazione e propagazione* (ciò solo per virus e worm): una volta eseguito, il malware tende a replicarsi ed a individuare nuovi obiettivi verso cui propagarsi.

4. *Azione malevole*: al verificarsi del compimento di una determinata azione, il codice virale esegue i propri compiti malevoli, come distruzione o furto dei dati del sistema.

È possibile distinguere i malware in due distinte macro categorie:

- quelli che per poter essere eseguiti necessitano di un appropriato programma ospite	- comuni virus - cavalli di troia c.d. trojan - backdoor
- quelli che per poter essere eseguiti non hanno bisogno di alcun programma ospite, essendo del tutto autonomi	- worm - zombie - rootkit

Il *Trojan horse*, letteralmente cavallo di Troia (chiaro riferimento all'inganno della mitologia omerica), può essere definito come un "programma apparentemente utile, ma che contiene funzioni nascoste atte ad abusare dei privilegi dell'utente che lo esegue".

A differenza dei virus non ha la capacità di autoriproduzione e diffusione, ma è l'utente a scaricarlo. Di solito si presenta sotto forma di gioco, screensaver ed altri articoli di interesse, ma una volta eseguito, il trojan installa segretamente il file server sul computer della vittima, compiendo allo stesso tempo tutte le operazioni di "copertura" che si suppone debba compiere.

È proprio l'apparente inoffensività e il corretto funzionamento del programma che fa da "cavallo" e rappresenta il punto di forza dei trojan, che spesso attivano la connessione ad un server maligno scaricando così altri malware per infettare il PC ed assumere il controllo completo del computer.

I *Worm* sono programmi software dannosi sviluppati per diffondersi il più rapidamente possibile dopo che il PC è stato infettato. A differenza dei virus, non sfruttano la presenza di altri programmi per moltiplicarsi, ma sfruttano i dispositivi di memorizzazione come le chiavette USB, le e-mail o le vulnerabilità nel sistema operativo. La loro propagazione rallenta le prestazioni dei PC e delle reti, diffondono dati all'esterno e possono provocare problemi al funzionamento generale del PC.

Tuttavia se un tempo erano i virus a seminare il panico, poi è arrivato lo *spam* che rappresenta circa l'80% del traffico complessivo sulla Rete: ed è nato così lo spammalware.

Come ultima frontiera dei pericoli digitali non possono essere dimenticati i micidiali "*Ransomware*" programmi maligni che, utilizzando efficaci tecniche di cifratura dei file, rendono inutilizzabili documenti, archivi, immagini e qualunque altro contenuto venga memorizzato sul disco fisso. L'operazione criminale è il preludio di una manovra estorsiva che si realizza con il rilascio di una salvifica parola chiave a fronte del pagamento di una determinata somma: "ransom", infatti, è il termine anglofono che identifica il riscatto.

Ultimamente "wannacry" ha creato non pochi danni sia nel settore pubblico che in quello privato, ma per il passato anche "cryptolocker" è stato l'incubo di molti utenti della rete e di molti studi professionali.

Ma oltre alle varie famiglie di virus non possono essere dimenticate come attacchi provenienti dal Web le varie forme di frode informatica come il phishing che è un tipo di frode ideato proprio allo scopo di rubare l'identità di un utente.

Quando viene attuato, una persona malintenzionata cerca di appropriarsi di informazioni quali numeri di carta di credito, password, informazioni relative ad account o altre informazioni personali convincendo l'utente a fornirgliele con falsi pretesti.

In concreto il phishing viene messo in atto da un utente malintenzionato che invia milioni di false e-mail che sembrano provenire da siti Web noti o fidati come il sito della propria banca o della società di emissione della carta di credito.

I messaggi di posta elettronica e i siti Web in cui l'utente viene spesso indirizzato per loro tramite sembrano sufficientemente ufficiali da trarre in inganno molte persone sulla loro autenticità. Ritenendo queste e-mail attendibili, gli utenti troppo spesso rispondono ingenuamente a richieste di numeri di carta di credito, password, informazioni su account ed altre informazioni personali.

Per far sembrare tali messaggi di posta elettronica ancora più veritieri, un esperto di contraffazione potrebbe inserirvi un collegamento che apparentemente consente di accedere ad un sito Web autentico, ma che di fatto conduce ad un sito contraffatto o persino una finestra a comparsa dall'aspetto identico al rispettivo sito ufficiale.

Queste imitazioni sono spesso chiamate siti Web "spoofed".

Una volta all'interno di uno di questi siti falsificati, si possono immettere involontariamente informazioni ancora più personali che verranno poi trasmesse direttamente all'autore del sito che le utilizzerà per acquistare prodotti, richiedere una nuova carta di credito o sottrarre l'identità dell'utente.

Altra tecnica simile al phishing è il pharming che è una tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato ed indirizzato direttamente verso un server Web clone che lo porterà a rivelare inconsapevolmente a sconosciuti i propri dati sensibili, come numero di conto corrente, nome utente, password, numero di carta di credito.

Proprio avuto riferimento a queste forme di frode informatica di recente con il D.L. 14 agosto 2013, n. 93, convertito dalla Legge 15 ottobre 2013, n. 119 è stata introdotta, per la prima volta, nel codice penale, la nozione di "identità digitale", prevedendo un'aggravante per il delitto di frode informatica (art. 640-*ter*), "se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti". Si tratta per di più di un'aggravante a effetto speciale, in quanto prevede la pena della reclusione da due a sei anni e della multa da euro 600 a euro 3.000.

Ma il web presenta anche altre insidie sebbene dalle caratteristiche un po' particolari. Si tratta del cosiddetto *Dark web* di cui si parla tanto negli ultimi tempi.

Ogni volta che accediamo al nostro profilo Facebook privato, quando guardiamo la nostra casella di posta elettronica via web oppure ci colleghiamo al nostro conto corrente on line. Ecco, in tutti questi casi siamo nel Deep Web, cioè quella parte di Internet che i motori di ricerca per varie ragioni non riescono a indicizzare, perché il loro sistemi di ricerca automatizzati non possono raggiungere i siti che lo compongono per una qualsiasi ragione. Nei casi citati, il fatto che i sistemi siano protetti da uno username e una password li rendono di fatto inaccessibili a Google & Co. Tuttavia esiste un altro luogo che, per ragioni diverse, risulta non catalogabile dai motori di ricerca; una porzione estremamente piccola rispetto al web e al deep web. Si tratta del Dark web.

Nel contesto generale di Internet si tratta di una manciata di siti, i ricercatori ipotizzano qualche centinaio di migliaia. Queste reti, costruite nell'ambito della Grande Rete, sono accessibili soltanto grazie a particolari software e la più celebre è conosciuta come TOR. Sostanzialmente si tratta di un network in cui la navigazione avviene attraverso l'omonimo browser

che dovrebbe garantire la navigazione anonima grazie alle caratteristiche peculiari del sistema di navigazione.

Il meccanismo di funzionamento prevede diversi strati di protezione, da cui il concetto di "*onion*" che significa cipolla, per impedire l'intercettazione del contenuto del traffico dati e l'identificazione di mittenti e destinatari. Le comunicazioni, infatti, sono crittografate e, prima di arrivare a destinazione, rimbalzano tra diversi sistemi, impedendone la tracciatura.

Naturalmente i pericoli in materia di sicurezza sono notevoli, difatti si stima che circa il 60% delle attività sul dark web sia illegale e spazi dalla pedo-pornografica fino al traffico di armi, passando attraverso quello della droga e la possibilità di affittare un killer.

Infine, per ultimare la breve rassegna dei rischi provenienti dal web o comunque dalla Rete in termini più generali non si può fare a meno di parlare di *cloud computing* inteso come l'insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto al cliente, di memorizzare/archiviare e/o elaborare dati grazie all'utilizzo di risorse distribuite e accessibili in rete.

Il *cloud* rappresenta per le sue caratteristiche la soluzione ottimale per molte aziende grandi e piccole, che hanno bisogno ciclicamente di notevoli risorse e che non sono in grado di sostenerne gli ingenti costi. Indubbiamente, per le stesse ragioni, anche gli studi professionali possono trarre diversi vantaggi dall'utilizzo del *cloud* la cui diffusione su larga scala consentirebbe il superamento dell'assetto attuale, caratterizzato da una miriade di client remoti, dotati di una propria autonoma postazione o di propri server "*in house*" in favore di un regime di "Software as a Service" (o "Storage as a Service"), consistente nel servirsi di software e hard disk messi a disposizione dai gestori delle nuvole e accessibili tramite browser web. Non più programmi da far girare né dati da archiviare su singoli pc, ma grossi sistemi integrati, indefiniti, di server e processori, dai quali attingere capacità di memoria e di processo a seconda delle proprie esigenze.

Naturalmente, però, c'è sempre un rovescio della medaglia ed il *cloud computing*, per quanto molto appetibile, comporta due grossi inconvenienti:

- perdita del controllo dei propri dati;
- concentrazione dei dati nelle mani di pochi soggetti.

In effetti le principali criticità del *cloud computing* riguardano il tema della sicurezza dei dati. L'attuale normativa europea ha da tempo introdotto (per le imprese e per i loro *outsourcer* informatici) l'obbligo di garantire la riservatezza, l'integrità e la disponibilità dei dati. È come se i dati fossero "in prestito" alle imprese: queste ultime devono proteggerli adeguatamente, valutando in anticipo quali sono i rischi che incombono sugli stessi, e poi predisponendo contromisure efficaci. Questo obiettivo viene perseguito con metodologie differenti dai vari Paesi europei: alcuni lasciano le imprese libere di attenersi alle metodologie definite dagli standard internazionali di

data security; altri (fra cui l'Italia) definiscono precisi standard normativi (nel nostro ordinamento, le cosiddette "misure minime di sicurezza").

7. Le applicazioni nel settore mobile

Da tempo ormai i device (smarhphone, tablet ecc.) sono diventati parte integrante della nostra vita. Negli ultimi anni sono poi nate le APP o applicazioni per device mobili, che ci consentono di svolgere moltissime attività: conoscere il ritardo del treno, verificare disponibilità di alberghi, aggiornamenti professionali, e tanto altro ancora.

Sostanzialmente, l'APP è un'applicazione software progettata per consentire di interagire con le informazioni e gli strumenti su cui è installata. In effetti l'APP non è altro che l'abbreviazione del termine "applicazione" ed è indicativo di un software contraddistinto da semplificazione ed eliminazione del superfluo le cui caratteristiche principali, pertanto, sono leggerezza, essenzialità e velocità, anche in considerazione delle limitate risorse hardware dei dispositivi mobili (smartphone, tablet, lettori mp3, smartwatch, etc.) i quali utilizzano batterie e processori meno potenti rispetto ai personal computer. Un'altra caratteristica delle APP è la loro capacità di poter interagire totalmente sia a livello software sia hardware del dispositivo mobile sul quale vengono installate aumentandone così le possibilità di utilizzo e gestione: ad esempio display, fotocamera, funzionalità di geolocalizzazione, consumi, etc.

Le APP possono essere scaricate dagli appositi store o market dei quali dispone ogni sistema operativo mobile. A seconda del sistema operativo di destinazione, le APP sono create con l'apposito linguaggio di programmazione:

- Sistema operativo Android di Google utilizza come linguaggio di programmazione Java;
- Sistema operativo iOS di Apple utilizza come linguaggio di programmazione Objective-C, ma dal 2014 utilizza anche il nuovo linguaggio Swift che prenderà progressivamente il posto del vecchio Objective-C;
- Sistema operativo Windows Runtime di Windows utilizza vari linguaggi di programmazione, come C#, Visual Basic, C++ o Javascript.

Dagli albori ad oggi il numero delle applicazioni per dispositivi mobili ha avuto un trend di crescita continua: dalle 500 app disponibili al lancio dell'App Store di Apple si è arrivati a quota 1.500.000 applicazioni nel Google Play Store (inizialmente Google aveva a disposizione solo 50 app).

Le applicazioni coprono varie aree di interesse e possono essere raggruppate secondo diverse tipologie: possono essere distinte in base al prezzo, alla categoria di appartenenza, alla tecnologia applicata, etc.

Naturalmente tra i problemi giuridici che scaturiscono dallo sviluppo e dall'utilizzo delle APP rientrano quelli relativi al trattamento dei dati ed alla sicurezza trattati nella presente pubblicazione.

Il problema del corretto trattamento dati è stato ampiamente affrontato a livello comunitario dal Gruppo di lavoro *ex* art. 29 nel parere n. 2/2013.

Vediamoli per punti.

A) *Legge applicabile*.

Un primo aspetto esaminato dal Gruppo di Lavoro riguarda l'individuazione del diritto applicabile alle APP. Possiamo infatti avere l'interessato (ovvero il soggetto che usa la APP e a cui i dati si riferiscono) in uno Stato, lo sviluppatore in un altro Stato, il produttore ubicato in un altro Stato ancora, etc.

Come è noto a livello comunitario attualmente si applica ancora la Direttiva sulla protezione dei dati (95/46/CE) a cui si aggiungono la Dir. e-privacy (2002/58/CE, modificata dalla Dir. 2009/136/CE), tutte attuate in Italia dal D.Lgs. n. 196/2003, ma a breve diventerà obbligatorio il Regolamento UE 2016/679.

In ogni caso la normativa comunitaria troverà applicazione ogni qualvolta una parte coinvolta nello sviluppo, nella distribuzione e nel funzionamento di applicazioni sia qualificata responsabile del trattamento e si trovi in uno Stato dell'UE. Non è tuttavia l'unico requisito. La normativa comunitaria si applica anche quando, per il trattamento dati, il Responsabile NON si trova nel territorio UE, ma si ricorre a strumenti situati nel territorio UE.

B) *Correttezza del trattamento*.

Dal punto di vista della correttezza del trattamento dati il Gruppo di Lavoro ex art. 29 pone l'attenzione su alcuni trattamenti in particolare.

Innanzitutto evidenzia la necessità di identificare i ruoli dei soggetti coinvolti. Normalmente nella realizzazione di una APP possiamo trovare gli sviluppatori, i produttori della APP, le APP store o i rivenditori e le parti terze come gli sponsor, ma nel caso di APP mediche potremmo avere anche gli operatori sanitari.

C) *Consenso al trattamento*.

Conditio sine qua non di qualsiasi trattamento dati, resta poi il consenso preventivo all'installazione e al trattamento di dati personali dell'interessato.

Nel caso di una qualsiasi APP, il principale fondamento giuridico applicabile è il consenso, poiché con l'installazione di un'applicazione, nel dispositivo dell'utente finale vengono inserite delle informazioni e spesso le stesse APP accedo ai dati memorizzati sul dispositivo.

D) *Autorizzazione al trattamento*.

Per quanto riguarda il trattamento di dati sensibili, si ricorda che attualmente l'art. 26 del Codice per la protezione dei dati personali (ma anche il Regolamento UE è orientato in tal senso) richiede anche l'autorizzazione del Garante al trattamento dati. Si ricorda che esistono delle autorizzazioni generali come la n. 2/2016 (per i dati sensibili) che consentono il trattamento dati sensibili a particolari categorie di dati.

E) *Misure organizzative e tecniche*.

Il Gruppo di lavoro, evidenzia l'obbligo per titolari e responsabili del trattamento di adottare misure organizzative e tecniche per garantire la protezione dei dati personali.

Naturalmente le misure devono essere prese da tutti i soggetti coinvolti e, ancora una volta, è importante stabilire ruoli e responsabilità per individuare gli obblighi di ciascuno.

F) *Dati genetici e biometrici*.

Da ultimo si segnalano particolari cautele per il trattamento di dati genetici e biometrici.

8. Come difendersi dai virus e, in particolare, dalle nuove generazioni di virus (Ransomware)

Purtroppo l'Italia è tra i paesi più colpiti dai virus informatici ed in particolar modo dai Ransomware. Si registrano continui casi di infezione a danno di PC privati come per importanti infrastrutture nel settore privato e nel pubblico, pertanto si ritiene di fare cosa utile nel fornire indicazioni a tutti gli studi professionali al fine di prevenire tale tipologia di infezione e non perdere i propri dati.

1) Prestare la massima attenzione ai messaggi di posta elettronica.

Solitamente il malware viene veicolato attraverso email contenenti allegati malevoli e indirizzati ad account di posta di privati ed aziende. Il corpo della mail è preparato ad arte e facendo leva sull'importanza del documento recapitato all'utente, lo invita a scaricare o visualizzare il file proposto che di solito riguarda un fantomatico riscontro su spedizioni, ordini, fatture o bollette.

Al fine di non incappare in questa tipologia di malware è bene verificare, ove possibile, che:

- il dominio della casella di posta del mittente abbia una corrispondenza con l'entità (azienda, ente, società o persona) scrivente;
- il nome dell'allegato non termini con un'estensione del tipo: .EXE, .JS, .CMD, .BAT, .SCR, .JAR, .PIF, .COM, .PS1, .PS2, REG, .LNK, .INF .DLL, .MSC, .MSI, .HTA, .MSP;
- se il file allegato si riferisce ad un documento Microsoft Office con macro attivata (.DOCM, .DOTM, .XLSM, .PPTM) si consiglia di disabilitare l'esecuzione automatica delle macro e verificare l'attendibilità del documento.

In genere è bene prestare attenzione a tutti i file allegati inclusi in archivi di tipo .ZIP o .RAR poiché potrebbero contenere all'interno altre tipologie di file malevoli.

2) Abilitare la visualizzazione delle estensioni in Windows.

Nativamente i sistemi operativi Microsoft Windows nascondono le estensioni dei file impedendo all'utente di verificare visivamente la reale

natura del documento. In diverse occasioni Cryptolocker ha sfruttato questa impostazione per ingannare l'utente, ragione per cui si consiglia di cambiare le impostazioni di sistema deselezionando la casella di controllo "Nascondi le estensioni per i tipi di file conosciuti" raggiungibile da "Pannello di controllo" -> "Aspetto e personalizzazione" -> "Opzioni cartella".

3) Limitare l'accesso alle risorse di rete.

Alcune varianti di Ransomware con componente di cifratura sono in grado di controllare anche le risorse di rete (cartelle condivise sia in lettura sia in scrittura). Il malware, nel caso in cui i permessi utente lo consentano, è in grado di cifrare i documenti contenuti nelle cartelle condivise anche se la cartella è fisicamente presente su un altro PC non infetto. Per questo motivo è necessario evitare di rendere permanente il collegamento a cartelle di rete contenenti documenti di vitale importanza.

4) Fare copie di backup periodiche dei dati personali su dispositivi fissi o mobili.

È preferibile salvare su un hard disk esterno i documenti sensibili, è buona norma collegare l'hard disk su un computer senza accesso alla rete internet e su dispositivi di cui si è certi di non aver precedentemente eseguito azioni che potrebbero aver compromesso il sistema.

Si raccomanda di scollegare sempre il disco esterno non appena concluso il backup e riconnetterlo solo all'occorrenza, come nel caso di successivi backup o per il ripristino dei dati. Valutare inoltre l'utilizzo di software o dispositivi NAS con funzionalità automatiche di rilascio del disco esterno qualora conclusa l'attività o che predispongano l'inserimento di una password per l'accesso allo storage.

5) Utilizzare un buon sistema antivirus eseguendo regolari e giornalieri aggiornamenti del prodotto.

Si rammenta che la protezione antivirus, regolarmente attiva e funzionante, rimane un valido deterrente limitatamente alle minacce note ma non consente di ripristinare dati sottoposti a cifratura.

6) Mantenere aggiornato tutto il software.

È buona norma eseguire controlli periodici al fine di verificare l'eventuale rilascio di aggiornamenti di sicurezza del sistema operativo e dei singoli programmi successivamente installati.

7) Se possibile, utilizzare un personal firewall.

Il firewall, nativamente disponibile in molti sistemi operativi, dovrebbe essere configurato in modo da consentire la connessione verso internet solo alle applicazioni strettamente necessarie; così da impedire che eventuali programmi e/o malware possano scaricare autonomamente codice malevolo.

In generale vale la regola di non eseguire file di dubbia provenienza e di operare sul sistema con privilegi utente limitati, ad ogni modo le indicazioni sopra riportate non possono garantire una protezione completa contro

questa tipologia di virus, per cui si consiglia a tutti gli studi professionali sempre la massima prudenza.

9. Ulteriori consigli pratici per evitare truffe informatiche

1. Bisogna proteggere sempre la propria password. Mai divulgarla e cambiarla periodicamente, almeno ogni 3 mesi. È opportuno, inoltre, utilizzare sempre il numero massimo di caratteri che vengono messi a disposizione dal sistema. In questo modo si rende più difficile la violazione da parte dei programmi che decriptano password. Possibilmente non bisogna usare parole di senso compiuto, è fondamentale la combinazione di minuscole, maiuscole, numeri e caratteri speciali ($@#). Non bisogna legare la password a parole della propria vita privata o a date di nascita di familiari. Infine la password va cambiata per ogni account e va subito modificata quella assegnata inizialmente in automatico.

2. Prima di inserire i dati personali in un modulo o in una pagina web, bisogna verificare la presenza di indicatori che ne attestino la sicurezza (ad esempio che l'indirizzo contenga la scritta https e il simbolo del lucchetto chiuso accanto). Per comunicazioni riservate deve essere utilizzato software di cifratura per criptare un documento (ve ne sono tanto gratuiti scaricabili dalla rete come: Drag'n Crypt ULTRA, ProtectFile, PixelCryptor, FileDecoder, ecc.). Nei social e nelle chat non vanno mai divulgate informazioni sensibili come il nome, l'indirizzo, il numero telefonico, il numero di conto o la password.

3. Bisogna prestare molta attenzione alle informazioni personali quando si accede ad internet utilizzando una rete che non si conosce o di cui non si è sicuri (ad esempio una rete Wi-Fi gratuita in un locale pubblico). Con queste reti, chiunque nelle vicinanze, infatti con conoscenze informatiche adeguate potrebbe monitorare le informazioni trasmesse tra il computer/smartphone e l'hotspot Wi-Fi. Inoltre se si possiede una rete Wi-Fi a casa, bisogna proteggerla con una password sicura per evitare che altre persone la possano violare.