CYBER SECURITY
A TUTELA DEI DATI PERSONALI

Indice

1. Introduzione. Vita reale e vita virtuale; i due mondi che si fondono.

Nell'ultimo decennio siamo stati i protagonisti di un'evoluzione diversa da quella tradizionalmente studiata e conosciuta, ma di eguale importanza storica.
Con un semplice click riusciamo oggi a navigare ovunque senza alcun confine arrivando a conoscere la vita, i pensieri, i gusti, i costumi e le idee di persone che vivono dall'altra parte della terra, il tutto in tempo reale!
La tecnologia ormai è parte integrante del nostro presente, grazie alla stessa oggi possiamo da un lato creare un proprio profilo virtuale con cui interagire e dall'altro programmare e organizzare in maniera ottimale la nostra vita, ad esempio aprendo un conto online, prenotando una visita medica o richiedendo delle agevolazioni e/o bonus, e ciò è realizzabile solo inserendo, o meglio condividendo, virtualmente i nostri dati personali.
Da ciò che mangiamo, alle nostre vacanze, da ciò che facciamo nel nostro tempo libero a ciò che pensiamo, tutto ciò che proietta i nostri bisogni, le nostre esigenze anche le nostre curiosità, viene oggi proiettato su questo "mondo digitale". Con un processo graduale ma inarrestabile, siamo diventati protagonisti di quella che in maniera quasi infantile consideriamo una doppia vita, quella reale e quella virtuale, senza renderci conto invece che quest'ultima è ormai pregnante della nostra quotidianità e quindi parte integrante della nostra vita reale. Di questo dobbiamo imparare ad essere consapevoli, facendo quindi attenzione a ciò che comporta.

2. Cyber security. Proteggersi nella nostra realtà digitalizzata

Il mondo del digitale presenta numerosi ostacoli e cela pericoli che non sempre l'utente è in grado di riconoscere o aggirare, arrivando a rendersi personaggio principale di situazioni che ledono i propri diritti ed interessi.
Di seguito, se da un lato si tratterà il fenomeno della cyber security arrivando ad esplicare cosa si intende con tale espressione e le garanzie giuridiche legate a quest'argomento, dall'altro, si arriveranno a delineare due profili differenti, uno legato alla tutela dell'utente del web e alla protezione dei dati personali dello stesso, e l'altro in grado di fornire

un'elencazione di accorgimenti e accortezze che possono essere osservate da coloro che navigano sul web.
La nostra quotidianità, intesa in termini di bisogni, oggi più che mai e specie con riferimento all'attuale contesto storico, è contenuta in un mondo digitale, parallelo e collegato a quello reale, dove riversando tutte le nostre richieste, domande, sentendoci schermati e al sicuro, condividiamo con tutti le nostre idee, sensazioni o pensieri arrivando anche a condividere i nostri dati più personali.
Strettamente conseguente al fenomeno del web e della dipendenza da questo, vi è il tema della cyber security, noto anche con il nome di sicurezza informatica, ossia l'insieme di quelle attività, strumenti e regole, tese da un lato a difendere il dispositivo informatico, come ad esempio, pc, smartphone o tablet, e dall'altro a tutelare i dati sensibili, ossia i nostri dati personali, da eventuali minacce, come il furto degli stessi da parte di soggetti terzi, o da vere e proprie truffe di carattere economico.
Nel momento esatto in cui decidiamo di utilizzare un dispositivo informatico, richiedendo l'accesso a determinati servizi, anche non per forza ludici come ad esempio quelli legati all'attività della pubblica amministrazione, ci viene chiesto di creare un proprio profilo dove dobbiamo condividere i nostri dati personali, come l'indirizzo di residenza, il numero di telefono o anche semplicemente il nostro indirizzo di posta elettronica. In parole semplici, ogni qualvolta accediamo su di una piattaforma digitale siamo chiamati a compilare moduli dove dobbiamo inserire le nostre generalità, sottoscrivendo le informazioni che ci vengono chieste, fleggando, attraverso una lettera informativa di politica di sicurezza interna, che analizzeremo in seguito, al fine di poter arrivare a creare il profilo.
Ma, una volta inserite tutte queste informazioni, le stesse dove vanno a finire e soprattutto chi controlla come i nostri dati vengano gestiti e utilizzati nelle diverse piattaforme dove sono stati registrati?
Ebbene, per rispondere a queste domande, dobbiamo analizzare la cyber security come metodo volto a salvaguardare le informazioni e gli strumenti informatici, rispetto a tre parametri fondamentali quali: riservatezza, integrità e disponibilità, il cosiddetto RID.

Per riservatezza si intende garantire l'accesso alle informazioni esclusivamente ai soggetti

che hanno diritto ad accedervi in quanto autorizzati a farlo. La riservatezza alle informazioni dei dati deve essere garantita durante tutto il ciclo di vita dell'informazione, ossia da quando viene generata e raccolta a quando viene distrutta, passando ovviamente per ogni tipo di conservazione in una banca dati. Ad esempio, se un dato classificato come segreto viene invece accidentalmente visto da soggetti non autorizzati a visionarlo, in questo caso si configura una violazione della riservatezza.
Si parla di integrità quando ci si riferisce alla caratteristica dell'informazione di non essere in alcun modo alterata o corrotta. In questo caso stiamo parlando di ogni evento che può alterare e corrompere le informazioni, e quindi ad esempio una modifica accidentale di una informazione, o la corruzione della stessa che può avvenire per ipotesi con il guasto ad un supporto di memorizzazione. I dati, così come trasferiti al soggetto autorizzato devono mantenersi integri per tutta la durata della loro conservazione e utilizzo all'interno della banca dati.
Per disponibilità si intende che una necessaria informazione deve essere accessibile in un determinato momento. Se tuttavia ciò non accade, il danno che ne può derivare è enorme. Pensiamo ad una sala operatoria e ad un chirurgo che deve accedere ai dati di un paziente per eseguire l'operazione e gli stessi non siano accessibili.
Dunque, la cyber security si pone con l'unico intento di difendere la nostra sfera virtuale da attacchi esterni mettendoci a riparo dagli stessi e dandoci la possibilità di poter rafforzare la nostra sicurezza nel mondo virtuale.
In questi anni si è parlato molto di cyber security, e molto è stato fatto per potenziarla, in maniera continuativa dato che le modalità attuate dai "malfattori" per eludere i vari sistemi di sicurezza viaggiano e si evolvono molto velocemente, ponendo seriamente a rischio la privacy degli utenti e di numerose aziende o società anche molto note, che periodicamente vedono manomessi i propri sistemi informatici interni e vengono "derubati" dei dati personali dei propri iscritti.

3. I cyberattack e i pirati contemporanei

I cyberattack, ossia gli attacchi informatici, sono attuati o da singoli soggetti o anche da

vere e proprie organizzazioni che, attraverso l'utilizzo di attività illegittime, ad esempio virus, tendono a colpire sistemi informatici, infrastrutture, reti di calcolatori di privati o aziende intrufolandosi furtivamente o nelle reti dati dei malcapitati, come accade con le cosiddette mail spam, o nei sistemi informatici specie aziendali, in maniera brutale arrivando a superare le difese della cyber security, forzando l'accesso di entrata e rendendo vulnerabili i vari sistemi della rete sino a giungere ai database, le banche dati dove sono elencati e custoditi i dati di ogni singolo utente.

Un esempio esemplificativo di quanto appena detto, è il fenomeno del phishing.

Il phishing è una vera e propria truffa informatica che si realizza e perfeziona nel momento esatto in cui riceviamo una mail relativa ad una comunicazione, con tanto di logo contraffatto ad esempio del nostro istituto di credito, che ci invita a fornire dati riservati (numero di carta di credito o password di accesso al servizio di home banking) motivando tale richiesta con ragioni di ordine tecnico o per un aggiornamento dei dati. L'utente, proprio perché tratto in inganno dalla presenza del logo della società o dell'azienda, crede che sia effettivamente una comunicazione da parte di quest'ultima arrivando a cliccare sul link indicato senza rendersi conto di dare così accesso al proprio pc.

Questo fenomeno negli ultimi anni ha fatto registrare numerose vittime tanto tra gli utenti quanto tra le aziende. Proprio le aziende sono state "attaccate" e spogliate tanto dei propri loghi quanto dei dati dei propri utenti.

In parole più semplici, il phishing è una minaccia che sfrutta le mail per uno scopo di truffa, sia esso convincere le persone a cliccare su alcuni link che rimandano a siti web che contengono malware e spyware sia esso un sistema per recuperare i dati degli utenti (per esempio richiedono credenziali e password di accesso ad un sistema con la scusa che devono essere riconfermati o controllati dall'azienda da cui è apparentemente stata inviata la mail).

Come poc'anzi espresso, il phishing ha negli ultimi anni messo a segno numerose truffe a danno di numerosi utenti arrivando a mutare più volte il proprio nome (ad esempio oggi si tende a parlare di vishing e smishing) ma utilizzando sempre le stesse modalità di raggiro.

La truffa del phishing, negli anni ha mutato le proprie modalità di esecuzione, anche a causa di una campagna informativa ad hoc creata dalle stesse aziende e diretta ai propri utenti che ha reso difficile l'adescamento di quest'ultimi. Difatti oggi ad esempio, l'utente

non riceve una mail, che con calma può leggere e verificare anche chiamando il proprio istituto di credito per confermarne l'autenticità, ma bensì può ricevere una chiamata sul proprio telefono e il numero dal quale riceve la stessa, paradossalmente, risulta esser quello del proprio istituto di credito.
Negli ultimi tempi, molti istituiti di credito hanno avviato importanti campagne di informazione ai propri correntisti su questo tipo di truffe e su come evitarle, anche perché attraverso piccole accortezze si può prendere contezza di esser sotto tiro da parte di malfattori del web.

4. Banner e non solo

Mentre il phishing e le sue varianti sono particolari tipologie di truffa realizzata sulla rete internet attraverso l'inganno degli utenti, esistono pratiche commerciali scorrette che pur non configurandosi come un vero e proprio reato molte volte provocano ingenti danni in capo agli utenti.
Per meglio descrivere di che tipo di pratica si sta facendo riferimento, si voglia partire da un esempio. Vi è mai capitato di navigare con lo smartphone e la vostra attenzione viene catturata da un articolo in particolare? Ebbene, dopo che questa notizia riesce ad attirare l'attenzione del lettore, con messaggi anche molto semplici come ad esempio "sai quale marchio di pasta utilizza solo grano italiano", cliccando sul link indicato, in automatico vengono attivati sulla propria utenza telefonica uno o più abbonamenti a pagamento del tutto indesiderati. Sebbene riusciamo a disattivare l'abbonamento, arrivando anche a perdere determinate somme, i nostri dati vengono illegittimamente trattenuti da queste sconosciute aziende le quali continueranno periodicamente ad inviarci sulla nostra casella di posta elettronica comunicazioni pubblicitarie o peggio essere vittime di continue e quotidiane chiamate ai soli fini pubblicitari.
Al fine di tutelare i diritti di utenti e consumatori, ed anche innanzi alle sempre più raffinate tecniche utilizzate dai malfattori del web, prezioso è stato l'impegno da parte delle Associazioni dei consumatori che hanno prontamente ogniqualvolta segnalato alle opportune Autorità le pratiche poste in atto a danno degli utenti ed aiutando legalmente

tutte le vittime di queste truffe.

5. Una pioggia di cookie

Capita spesso che dopo aver fatto una ricerca on line nei giorni seguenti diverse pagine che poi visitiamo ci ripropongono lo stesso articolo ricercato. Anche dopo aver cercato quel determinato articolo su un'app, lo stesso ci viene riproposto poi in banner pubblicitari a costi inferiori.

Questo è possibile perchè ogni qualvolta navigando sul web e vogliamo consultare determinate pagine, ci viene chiesto di accettare la seguente formula «Abbiamo a cuore la tua privacy. Noi e i nostri partner archiviamo e/o accediamo alle informazioni su un dispositivo (come i cookie) e trattiamo i dati personali (come gli identificatori univoci e altri dati del dispositivo) per annunci e contenuti personalizzati, misurazione di annunci e contenuti, approfondimenti sul pubblico e sviluppo del prodotto. Con il tuo consenso, noi e i nostri partner possiamo utilizzare dati di geolocalizzazione e identificazione precisi attraverso la scansione del dispositivo. Informativa sulla Privacy».

Solo una volta aver accettato questa condizione possiamo usufruire delle informazioni contenute nell'articolo.

In tema di policy, non si può non far riferimento ai cookie e alla frase a cui ormai siamo più abituati e che siamo chiamati o meno ad accettare "accetta tutti i cookie di questa pagina," ma cosa sono? I cookie sono frammenti di dati sugli utenti memorizzati sul computer e utilizzati per migliorare la navigazione. I cookie, anche conosciuti come cookie HTTP, web, Internet o del browser, vengono creati dal server e inviati sui nostri browser. Lo scambio di informazioni consente ai siti di riconoscere il nostro computer o dispositivo e inviargli informazioni personalizzate in base alle nostre sessioni.

Spetta all'utente decidere se accettare o meno i -cookie. In teoria, i cookie sono una cosa buona. Personalizzare la navigazione significa offrire agli utenti un'esperienza più semplice e piacevole.

I dati salvati nei cookie non sono pericolosi di per sé, non sono un malware, il problema è il modo in cui i vari siti web possono utilizzare i dati, potenzialmente violando la privacy

dell'utente. I cybercriminali possono utilizzare le informazioni contenute nei cookie per estrapolare la cronologia della navigazione.
Ebbene, proprio al fine di non incappare in eventuali problemi l'utente deve essere in grado di saper conoscere cosa sono i cookie e saper distinguere tra quelli che possono essere in grado di aiutarci nella nostra ricerca e quelli che è preferibile bloccare, in base alle nostre necessità.
Nella maggior parte dei casi, i cookie sono utili dal momento in cui creano esperienze online più semplici e veloci memorizzando il login, il carrello della spesa, la lingua, la valuta e altre impostazioni personali. È sicuro utilizzarli sui siti affidabili, che in questo modo permettono all'utente di navigare in modo efficiente e personalizzato.
Tuttavia, il discorso muta laddove l'utente consente i cookie su siti sconosciuti e/o sospetti che potrebbero essere pericolosi per i dispositivi. Di per sé, i cookie non possono danneggiare un computer, ma possono aiutare gli hacker a infiltrarsi e recuperare le informazioni contenute nei cookie esponendo in maniera pericolosa l'ignaro utente.
Riassumendo in semplici parole, laddove l'utente decida di non accettare i cookie sarà chiamato ogni qualvolta decide di avviare una navigazione, a ricercare le varie informazioni, e non potrà navigare con impostazioni personalizzate, ma a parte questo disattivare i cookie non comporta nessun problema. Se per l'utente la cosa più importante è la privacy, come giusto che sia, lo stesso potrà provare a bloccare i cookie per evitare la raccolta di dati non autorizzata anche se bisogna ricordare che si tratta di un'eventualità piuttosto remota.
Detto ciò, nulla impedisce all'utente di rimuovere i cookie. Difatti, è una buona idea cancellare i cookie, più che altro perché in questo modo riduciamo il rischio di violazioni.
Ogni qualvolta navighiamo sul web dobbiamo prestare attenzione a cosa accettiamo dal momento in cui quello che per noi è un semplice click su di una casella è invece l'autorizzazione alla trasmissione dei nostri dati personali ad aziende terze ed ignote.

6. Mi autotutelo, ma come?

Alla luce di quanto espresso, risulta d'obbligo chiedersi, se questi hackers riescono ad accedere facilmente sui nostri profili, in particolar modo a quelli creati per i servizi postali

e bancari. Qual è l'errore che quotidianamente e ripetutamente commettiamo e che agevola questo tipo di truffe?
In realtà gli errori che tutti commettiamo sono anche i più banali.
Uno dei primi è quello di arrivare a creare chiavi di accesso, password, basate o sull'indicazione della propria data di nascita o composte seguendo una sequenza numerica banale, come ad esempio 1234e viceversa.
Utilizzare queste due formulazioni tipo fa si che in pochissimo tempo i cybercriminali possano entrare nella nostra area virtuale e rubare i nostri dati.
Tutte le chiavi di sicurezza alle quali attribuiamo queste due condizioni, ossia o la nostra data di nascita o una sequenza numerica, vengono infatti definite "deboli" dalla maggior parte dei sistemi informatici di raccolta dati.
Ebbene, al fine di tutelare i nostri dati, ogni qualvolta ci registriamo su di un nuovo servizio ci vien richiesta una password "forte" o "molto forte", proprio al fine di proteggere il proprio dispositivo e il proprio profilo da eventuali, e anche probabili attacchi esterni, viene richiesto l'inserimento di una sequenza alfanumerica composta da almeno otto caratteri e con la presenza anche di caratteri speciali (ad esempio: @; #; *; =).
Altro errore molto frequente e che dovremmo evitare, legato sempre alla chiave di sicurezza, è quello di utilizzare per ogni portale in cui si è registrati la stessa password; in questo caso nel momento in cui un hacker riuscisse a violare un nostro profilo, automaticamente potrebbe entrare indisturbato in tutti gli altri.
Laddove utilizziamo password forti e differenti per ogni profilo digitale che ci siamo creati, sarà sempre più difficile per gli hacker entrare sugli stessi e rubare i nostri dati.
Altro errore molto diffuso soprattutto tra gli utenti più giovani, è quello di collegarsi ad una rete Wi-Fi pubblica, ossia le connessioni libere poiché non protette. Queste sono un facile canale di accesso per gli hacker i quali possono intercettare la trasmissione dei dati degli utenti che si "agganciano" a quella linea. In questi casi è sempre consigliabile non inserire password e/o altre informazioni private, ed in particolar modo evitare di entrare sui propri profili bancari e/o postali mentre si naviga utilizzando il wi-fi pubblico.
La nostra sicurezza digitale non passa solo attraverso una semplice chiave di sicurezza ma, bensì, anche attraverso il mancato update, il cosiddetto aggiornamento, dei sistemi e delle

app nonché nell'ignorare i termini e le condizioni di un servizio.
Molto spesso quando scarichiamo una nuova app sul nostro dispositivo elettronico non prestiamo la ben che minima attenzione a quel riquadro che ci appare sullo schermo, molte volte ignorato perché i contenuti sono assai lunghi. Incoscientemente pensiamo che sia una cosa inutile da leggere e con molta celerità ci accingiamo a fleggare "acconsento" in modo tale da poter immediatamente utilizzate l'app .
A volte questa pigrizia di non leggere i contenuti prima di dare quel consenso, ci spinge a commettere un gravissimo errore!
Difatti, l'accettare i termini e le condizioni di un servizio senza leggere attentamente tutti i punti fa sì che, involontariamente, a volte accettiamo condizioni pericolose per la tutela dei nostri dati e della nostra privacy arrivando anche a permettere che i nostri dati sensibili possano essere condivisi a terze parti.
Dunque, sappiamo benissimo che questi documenti sono molto lunghi e noi non vediamo l'ora di usufruire di quel programma, ma questa abitudine è assolutamente sbagliata. Dobbiamo imparare a prestare la massima attenzione a ciò a cui "acconsentiamo" con quel semplice click, al fine di evitare che i malfattori del web possano aver libero accesso ai nostri dati.
Sempre in materia di app e di cattive abitudini da evitare, c'è quella di ignorare gli aggiornamenti richiesti dall'applicazione stessa.
Sul punto, gli esperti di sicurezza informatica raccomandano di installare subito gli update disponibili; gli aggiornamenti, infatti, consentono di bypassare eventuali falle di sicurezza informatica e di proteggere i dispositivi da aggressioni esterne. Ogni giorno vengono messi in rete migliaia di nuovi malware come virus, trojan o ransomware e uno dei modi per tutelarsi dalle cyber minacce è avere un pc o uno smartphone sempre aggiornato.
Ed ancora, di sicurezza informativa se ne parla anche in tema di backup e di controllo attento della casella di posta elettronica.
Il backup è un'operazione fondamentale che ci permette di tenere al sicuro i propri dati dagli imprevisti di tutti i giorni arrivando a creare una copia di sicurezza di file e cartelle che abbiamo presenti sui nostri dispositivi. Anche qui, gli esperti di sicurezza informatica consigliano di effettuare periodicamente il backup di dati e file mettendoli al riparo in un

posto sicuro. Pensiamo a cosa possa accadere se il nostro Pc viene preso di mira dagli hacker ed i nostri dati completamente rubati, ad esempio. Grazie al backup possiamo avere sempre una copia di tutti i documenti presenti sui dispositivi elettronici in nostro possesso.
E' molto importate fare dei backup periodici, i restore, al fine di controllare la funzionalità del recupero dei dati e contestualmente archiviare la documentazione in nostro possesso.
Ed ancora, molte volte l'utente vede recapitarsi delle comunicazioni sulla propria casella elettronica con l'invito a scaricare un determinato documento allegato al testo di cui non si conosce l'effettiva provenienza e/o la genuinità dello stesso.
Ricollegandoci alle modalità utilizzate nel phishing, potremmo ricevere una mail da un indirizzo di posta elettronica simile a quelli conosciuti ed utilizzati spesso, magari di colleghi e/o amici, in cui ci viene chiesto di scaricare il file allegato, molto spesso un documento di testo. In questi casi laddove non si presti la più accorta delle attenzioni, effettuando il download di quel documento cadiamo in una truffa, aprendo le porte nel nostro pc, della nostra casella di posta, a soggetti indesiderati che possono copiare/rubare tutte le informazioni presenti.
In tema di sicurezza informatica occorre sempre prestare la massima attenzione al fine di non incappare in truffe che possano danneggiare tanto il profilo dei dati personali quanto quello economico.
Quelli appena elencati possono essere dei piccoli, ma grandi, consigli che tutti gli utenti del web dovrebbero tenere a mente ogni qualvolta avviano una navigazione su internet o portano alla creazione di un profilo sui diversi portali.
A questi consigli, affianchiamo anche degli accorgimenti da seguire per non essere vittime di questi truffe e veder rubati i propri dati.
In prima battuta, su ogni dispositivo digitale in nostro possesso, sia esso un pc o uno smartphone, deve essere attivato un filtro antispam, il quale ci allerterà dell'eventuale pericolo a cui il nostro dispositivo e/o account è sottoposto.
Nel caso in cui invece, riceviamo comunicazioni moleste, tramite sms o mail, come accade alle vittime del phishing, dobbiamo prestare notevole attenzione dal momento in cui il nostro profilo potrebbe esser stato preso di mira e quindi si sta tentando in tutti i modi di

voler accedere ai nostri dati. In questo caso si possono attuare una serie di procedure al fine di tutelarci. Prime tra tutte occorrerebbe portare ad una modifica di tutte le password dei vari profili attivi a nostro nome, anzi sarebbe consigliabile modificare periodicamente la chiave di accesso di ogni profilo a prescindere da eventuali attacchi, proprio per evitare gli stessi.

Quando riceviamo una mail "sospetta" dobbiamo, per prima cosa, controllare il dominio del mittente ciò si rende necessario specie quando riceviamo una comunicazione da un'azienda o da una società. In questo ultimo caso occorre verificare se la mail del mittente rappresenti proprio quella della società e/o dell'azienda, prestando particolar attenzione nel momento in cui nella comunicazione giunta ci vien richiesto di cliccare su di uno specifico ed indicato link.

Al fine di tutelarci ma soprattutto al saper come farlo e quali mezzi abbiamo per farlo, fondamentale risulta essere il ruolo svolto dalle Associazioni a tutela dei consumatori, le quali in virtù dei propri ruoli hanno posto in essere una significativa campagna informativa a tutela dei diritti e degli interessi dei consumatori con l'unico intento di informare il consumatore medio in merito alle truffe. Cyber security è anche sinonimo di conoscenza. L'educazione degli utenti è una forma di conoscenza fondamentale che rientra nel novero del principio della sicurezza informatica.

Su di un binario parallelo a quella della conoscenza informatica viaggia la protezione, che come già detto, consiste nell'insieme dei meccanismi utilizzati per il controllo di accesso alle risorse che ci permette di prendere visione e conoscenza di come quella pagina della quale si vuol prendere visione o quel link che si vuol aprire non risultano essere protetti facendo sì che la richiesta alla loro apertura potrebbe esporci ad un grave rischio in tema di sicurezza.

Sulla base di queste informazioni, dunque, sembrerebbe sussistere la necessità di far sì che tutti coloro che navighino sul web, al di dell'utilizzo che ne facciano, siano in grado non solo di saper navigare ma anche, e soprattutto, di sapersi difendere dai rischi, facilmente evitabili solo utilizzando una ordinaria diligenza.

Forse, ad oggi, le aspettative sul ruolo e l'uso di tecnologie sempre più moderne ed all'avanguardia sono notevolmente elevate, in quanto siamo quotidianamente esposti

all'attenta sorveglianza di ogni nostra singola azione rimanendo, a volte, anche indifferenti alla presenza di strumenti elettronici che controllano le nostre azioni o di pagine web e/o App che richiedono costantemente di geo localizzare la nostra posizione. In altri termini, siam divenuti tutti protagonisti anonimi agli occhi di una meccanismo informatico e digitale che controlla ogni nostro singolo movimento.

7. La digitalizzazione del Paese

Nell'attuale contesto storico, che non richiede certo alcun tipo di presentazione, si è registrato un aumento di nuovi utenti che per la prima volta hanno approcciato al mondo del digitale. Difatti, e come ben noto, durante il periodo pandemico dal mondo del lavoro, al mondo dell'istruzione passando anche per i sostegni che venivano riconosciuti dallo Stato si richiedeva sempre una procedura prettamente digitale, o online, dove l'utente veniva chiamato a creare un proprio profilo al fine di poter vedere soddisfatte le proprie richieste. L'arrivare a far sì che ogni richiesta potesse essere gestita in maniera digitale è stato per il Nostro Paese un grande passo in avanti dal momento in cui è in atto un vero e proprio fenomeno di digitalizzazione nel mondo della Pubblica Amministrazione, che pian piano arriverà a coinvolgere tutti quei settori che richiedono una collaborazione trasparente, efficace e sicura tra Ente e collettività. A mero titolo esemplificativo, si possono qui richiamare due voci che rappresentano la giusta chiave di cooperazione tra amministrazione e cittadino, la carta di identità elettronica e lo Spid, ossia il Sistema Pubblico d'Identità Digitale che ci permette di accedere facilmente ed in brevissimo tempo ai servizi online tanto della Pubblica Amministrazione quanto dei privati aderenti.
Dunque, se da un lato l'arrivare a digitalizzare un'intera collettività veniva visto positivamente sotto il profilo della modernizzazione e dell'arrivar a creare quel concetto da sempre auspicato di un'amministrazione trasparente e diretta con l'utente richiedente, dall'altro si è registrata una percentuale assai preoccupante per l'utilizzo del digitale al fine di poter accedere ed usufruire di determinati servizi non certo utili per il bene comune ma lesivi per la persona.
Ma quali sono i mezzi che l'ordinamento giuridico mette a disposizione dell'utente per

tutelare la privacy nel cyber spazio?
Sicuramente la contromisura più importante per la privacy è rappresentata dal Generale data Protection o più semplicemente GDPR, divenuto applicabile in tutti gli Stati dell'Unione Europea il 25 maggio del 2018.
Il GDPR nasce da precise esigenze, come indicato dalla stessa Commissione Ue, di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trasferimento di dati personali dall'Ue verso altre parti del mondo. Si tratta poi di una risposta, necessaria e urgente, alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali sempre più avvertite dai cittadini dell'Unione.
In estrema sintesi col GDPR:
Si introduce il concetto di responsabilizzazione o accountability del titolare;
Si introducono importi più elevati per le sanzioni amministrative pecuniarie che variano nel massimo a seconda delle disposizioni violate;
Si introducono concetti di "privacy by design", nonché di approccio basato sul rischio e adeguatezza delle misure di sicurezza, di valutazione d'impatto e data breach;
Regole più rigorose per la selezione e la nomina di un responsabile del trattamento e di eventuali sub-responsabili;
Si introduce la previsione in alcuni casi tassativi di nomina obbligatoria di un Responsabile della protezione dei dati;
Si introducono regole più chiare su informativa e consenso;
Viene ampliata la categoria dei diritti che spettano all'interessato;
Vengono stabiliti criteri rigorosi per il trasferimento degli stessi al di fuori dell'Ue

Eccoci quindi giunti alla fine di quello che possiamo definire un viaggio a cavallo di due epoche una dove il mondo del digitale era solamente un qualcosa di prettamente ludico e lontano dalla realtà quotidiana, e l'altro legato a quello della digitalizzazione, dove come già detto, in ragione della trasparenza la realtà virtuale è messa a disposizione dell'utente e della pubblica amministrazione.
In questo percorso, se da un lato abbiamo potuto osservare cosa si intende per cyber

security dall'altra si è giunti ad osservare quale possono essere i pericoli della scarsa conoscenza. Abbiamo elencato alcuni semplici accorgimenti da tenere sempre a mente affinché non si incappi in qualche imbroglio, ed in ultimo, abbiamo osservato quali sono le possibile tutele.

Non si può arrivare a pensare che la tecnologia unita al mondo del digitale possa esser considerata come un qualcosa che se non dosato faccia male, anzi al contrario dobbiamo imparare ad utilizzare gli strumenti digitali perché con essi è possibile risolvere tanti problemi, l'importante è essere consapevoli sia delle enormi risorse che ci mettono a disposizione, sia degli innumerevoli rischi a cui la navigazione ci sottopone.

In conclusione, la sicurezza informatica, così come quella personale, richiede una tutela specifica: non possiamo permettere che utenti ignari dei pericoli del web si immettano sulla piattaforma senza formazione alcuna e diventino facili bersagli di soggetti e/o organizzazioni di soggetti che si pongono con l'unico scopo di ledere i diritti altrui.

Fondamentale, in questa formazione, deve essere il ruolo di cooperazione tra le Autorità competenti e le Associazioni a tutela dei consumatori e degli utenti le quali devono, cosa che han fatto sino ad oggi, offrire una giusta informazione e tutela per il consumatore attraverso campagne di sensibilizzazione sul tema, che diversamente da altri è in continua evoluzione.

al futuro dico si

INNOVAZIONE SERVIZI OPPORTUNITÀ

Realizzato nell'ambito delle iniziative a favore di consumatori e utenti per emergenza sanitaria da COVID-19 promosse dalla Regione Lazio, realizzate con Fondi Ministero Sviluppo Economico (riparto 2020)

ADUSBEF

ASSOUTENTI LAZIO APS

CODACONS

MOVIMENTO DIFESA del Cittadino LAZIO