CILD Coalizione Italiana Libertà e Diritti civili

PROTEGGI I TUOI DATI PERSONALI

Guida pratica per saperne di più

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu

CILD Coalizione Italiana Libertà e Diritti civili

Chi siamo

Nata nel 2014, la Coalizione Italiana per le Libertà e i Diritti civili (CILD) è una rete di 35 organizzazioni della società civile che lavora per difendere e promuovere i diritti e le libertà di tutti, unendo attività di advocacy, campagne pubbliche e azione legale. Le aree tematiche di cui CILD si occupa sono soprattutto diritti di migranti e rifugiati, discriminazioni, giustizia penale, libertà di espressione e privacy.

Perché questa guida

Questa guida è un'introduzione alla tutela dei dati personali. Si tratta di un tema vasto e articolato, che coinvolge molti aspetti della nostra vita quotidiana e che presenta numerosi rischi, di cui spesso non ci rendiamo conto.

Ogni dato relativo alla nostra persona, una volta aggregato con altre informazioni, può essere infatti usato da istituzioni pubbliche ed aziende private per compilare “un puzzle” con l'immagine della nostra persona, che diventa sempre più preciso man mano che vengono somministrati nuovi dati.

Questo puzzle può essere usato a molti scopi: per vendere prodotti sempre più personalizzati, ad esempio. Sembra non esserci niente di male, ma basta pensare alla quantità di email di spam che riceviamo ogni giorno per renderci conto che i nostri dati non sono in possesso solo di coloro a cui li abbiamo ceduti intenzionalmente. E se in realtà il prodotto fossimo proprio noi?

E se l’immagine di noi che viene creata dai nostri dati venisse un giorno utilizzata per discriminare? Può sembrare un’idea remota, lontana dalla nostra quotidianità, ma un mutuo negato o una rata dell’assicurazione che sale senza apparente motivo possono essere eventi molto, molto concreti.

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROMA - cild.eu - info@cild.eu

CILD Coalizione Italiana Libertà e Diritti civili

Come possiamo proteggere i nostri dati personali?

Innanzitutto attraverso una diffusione consapevole. Evitiamo di "regalare" i nostri dati in cambio di servizi non indispensabili o dal contenuto dubbio, come tessere che vengono utilizzate raramente o accesso a "club" semi-esclusivi offerti da aziende.

Utilizziamo consapevolmente i social network, evitando di pubblicare con alta frequenza fotografie personali o dei nostri cari, la nostra posizione geolocalizzata o altre informazioni che consentono di individuare preferenze sessuali, politiche, religiose.

Ricordiamo che la diffusione di immagini di terzi privati senza il loro preventivo consenso è un illecito civile, che si aggrava quando vengono diffuse foto di minori senza averne la responsabilità genitoriale (in ogni caso, anche quando genitori di minori, non è opportuno pubblicare foto di minori sui social network).

Cosa fa (e cosa non fa) questa guida

Questa guida è una delle attività del nostro programma Libertà civili nell'era digitale, che si concentra sulla difesa della libertà di espressione e del diritto alla privacy e al controllo dei propri dati personali, contro la sorveglianza di massa, la censura e altre pratiche che mettono a rischio le libertà civili.

Ci proponiamo di darvi una presentazione dei principali temi e rischi quando si parla di dati personali, con indicazioni su come tutelarli. L'argomento è cruciale anche in vista di un cambiamento molto importante nel mondo della privacy: l'entrata in vigore del regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679), con cui la Commissione Europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea, sia all'interno che all'esterno dei

confini dell'Unione Europea. Il testo inizierà ad avere efficacia il 25 maggio 2018. Il testo legislativo sarà, inoltre, integrato anche da nuove norme in materia di tutela della vita privata e dei dati personali nell'ambito specifico delle comunicazioni elettroniche, attualmente al vaglio presso il Parlamento Europeo.

Come detto, il tema è tanto ampio da non consentire una trattazione esaustiva di ogni singolo aspetto e caso possibile. Si tratta di un primo passo che servirà a orientarsi in un contesto complicato, e che verrà seguito da altre attività più specifiche su singoli aspetti del tema.

La guida è stata realizzata dall'avvocato Tommaso Scannicchio, fellow del programma Libertà Civili nell'Era Digitale.

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROMA - cild.eu - info@cild.eu

Indice

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu

Cosa sono i dati personali?

Secondo la normativa europea e italiana, e comunemente accettata da giurisprudenza e dottrina, sono dati personali le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

Quindi, non solo i tradizionali "documenti di identità" ma più in generale qualsiasi dato riferibile ad un individuo identificabile, anche in un secondo momento. Particolarmente importanti sono:

- i dati identificativi: che permettono l'identificazione diretta, come i dati anagrafici, i documenti personali e le immagini, ecc.;
- i dati sensibili: sono definiti in questo modo dalla legge tutti i dati che qualificano la personalità del soggetto nelle sue scelte più intime in quanto possono rilevare, anche solo potenzialmente, l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;
- i dati giudiziari: fanno parte dei dati sensibili ed in particolare possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la veste di imputato o di indagato (i c.d. carichi pendenti).

Anche tutte le informazione che consentono di monitorare gli spostamenti di un individuo, quali forme di geolocalizzazione fornite da smartphone o applicazioni,

fornendo informazioni sui luoghi frequentati e sugli spostamenti, sono considerati dati personali e quindi soggetti alle forme di tutela previste dalla legge.

Cos'è il diritto alla protezione dei dati personali?

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo tutelato in Italia dal Codice in materia di protezione dei dati personali (decreto legislativo 20 giugno 2003, n. 196), e in Europa dal nuovo Regolamento 2017/679, che inizierà ad avere efficacia il 25 maggio 2018. È un diritto fondamentale dell'individuo riconosciuto a livello europeo e internazionale dalla Carta dei Diritti Fondamentali dell'UE (art. 7 e 8), Convenzione Europea sui Diritti dell'Uomo (art. 8) e Dichiarazione Universale dei Diritti dell'Uomo (art. 12), oltre che da vari altri atti normativi italiani e internazionali.

In concreto tale diritto consente ad ogni individuo di pretendere che i propri dati personali siano trattati da terzi solo nel rispetto delle regole e dei principi stabiliti dalla legge.

Come si esercita questo diritto?

Ogni persona può tutelare i propri dati personali, in primo luogo, esercitando i diritti previsti dall'articolo 7 del Codice in materia di protezione dei dati personali[1]. In particolare, ogni interessato può presentare un'istanza al titolare[2] o al responsabile (se designato) del trattamento, senza particolari formalità. L'istanza può essere riferita, a seconda delle esigenze dell'interessato, a specifici dati personali, a categorie di dati o ad un particolare trattamento, oppure a tutti i dati personali che lo riguardano, comunque trattati.

---

[1] Codice in materia di protezione dei dati personali, Decreto legislativo 30 giugno 2003, n.196, Garante per la protezione dei dati personali:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248

[2] Modello esercizio diritti in materia di protezione dei dati personali, Garante per la protezione dei dati personali:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1089924

Nell'esercizio dei diritti l'interessato può farsi assistere da una persona di fiducia (ad esempio un legale) e può anche conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi.

Il titolare del trattamento è obbligato a fornire una risposta ad ogni richiesta, senza ritardo, entro e non oltre:

- 15 giorni dal suo ricevimento;
- 30 giorni, se le operazioni necessarie per un integrale riscontro sono di particolare complessità, ovvero se ricorre altro giustificato motivo. In questo secondo caso, il titolare o il responsabile devono comunque dare riscontro all'interessato entro i primi 15 giorni.

Cosa fare se la risposta a un'istanza secondo l'articolo 7 del Codice non arriva nei tempi indicati o non è soddisfacente?

Se la risposta ad un'istanza con cui si esercita uno o più dei diritti previsti dall'articolo 7 del Codice in materia di protezione dei dati personali non arriva nei tempi indicati o non è soddisfacente, l'interessato può far valere i propri diritti dinanzi all'autorità giudiziaria o rivolgendosi al Garante per la protezione dei dati personali (vedi sezione successiva).

Tutelare il diritto alla protezione dei dati personali

Il Garante Italiano

Il Garante si occupa di verificare la correttezza del trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali in ambito pubblico e privato.

Si occupa, tra le altre cose di controllare che i trattamenti di dati personali siano conformi a leggi e regolamenti ed esaminare reclami e segnalazioni da parte degli utenti. Inoltre, ha il potere di vietare in tutto od in parte il trattamento di dati personali che per la loro natura, per le modalità o per gli effetti del loro trattamento possano rappresentare un rilevante pregiudizio per l'interessato e sanzionare eventuali illeciti.

Può adottare i provvedimenti previsti dalla normativa in materia di dati personali, tra cui, in particolare, le autorizzazioni generali per il trattamento dei dati sensibili, e segnalare al Governo, quando ritenuto opportuno, la necessità di adottare provvedimenti normativi specifici in ambito economico e sociale, anche partecipando attivamente alla discussione su iniziative normative con audizioni presso il Parlamento, svolgendo indagini conoscitive sullo stato di attuazione delle leggi in determinati settori e alle verifiche d'iniziativa sui trattamenti che, in base a specifici elementi, si abbia motivo di ritenere siano effettuati in violazione di legge o di regolamento. Il Garante, inoltre, prende parte alle attività comunitarie ed internazionali di settore, anche quale componente del Gruppo Articolo 29 e delle Autorità comuni di controllo previste da convenzioni internazionali (Europol, Schengen, Sistema informativo doganale).

Il ricorso al Garante

Il ricorso al Garante è un atto di denuncia da parte del privato, alternativo all'esercizio degli stessi diritti di fronte all'autorità giudiziaria.

È possibile ricorrere solo per far valere i diritti stabiliti all'articolo 7 del Codice in materia di protezione dei dati personali e solo quando la risposta del titolare del trattamento all'istanza con cui si esercitano i diritti non perviene nei tempi indicati o non è ritenuta soddisfacente, oppure il decorso dei termini previsti esporrebbe il soggetto richiedente ad un pregiudizio imminente ed irreparabile.

Il ricorso non è gratuito!

Al ricorso va, infatti, allegata la prova del versamento dei diritti di segreteria pari ad euro 150,00.

Non è possibile chiedere il risarcimento del danno in sede amministrativa di fronte al Garante. Le pretese risarcitorie possono essere fatte valere solo innanzi al giudice ordinario in Tribunale.

Il ricorso può comportare una condanna alle spese anche per il richiedente! A conclusione del procedimento instaurato dal ricorso, se una delle parti lo ha richiesto, il Garante determina l'ammontare delle spese e dei diritti inerenti al ricorso e lo pone a carico, anche solo in parte, della parte soccombente.

Il Garante può compensare le spese, anche parzialmente, se ricorrono giustificati motivi.

Il Garante ha fissato la condanna alle spese in misura forfettaria nell'importo minimo di euro 500,00 aumentabile sino ad un massimo di euro 1.000,00 in ragione della eventuale complessità dei singoli procedimenti.

Il reclamo al Garante

Il reclamo al Garante è un atto circostanziato con il quale si rappresenta una violazione della disciplina rilevante in materia di protezione dei dati personali.
Al reclamo segue un'istruttoria preliminare e un eventuale successivo procedimento amministrativo formale che può portare all'adozione di vari provvedimenti.
È possibile utilizzare il modello predisposto dal Garante sul proprio sito.[3]

La segnalazione al Garante

Quando non è possibile o non si vuole presentare un reclamo circostanziato (in quanto, ad esempio, non si dispone delle notizie necessarie), si può inviare al Garante una segnalazione, fornendo elementi utili per un eventuale intervento dell'Autorità volto a controllare più genericamente l'applicazione della disciplina rilevante in materia di protezione dei dati personali.

La segnalazione è gratuita e può essere proposta in carta libera e non è necessario seguire particolari formalità. Il Garante non è obbligato a pronunciarsi ovvero ad aprire indagini di alcun tipo in conseguenza di una o più segnalazioni.

Il Garante Europeo

Il Garante Europeo ha il compito principale di controllare che le istituzioni e gli organi dell'UE rispettino il diritto dei cittadini al trattamento riservato dei dati personali.

In aggiunta a questo compito fondamentale, offre consulenza alle istituzioni e agli organi dell'UE su tutti gli aspetti del trattamento dei dati personali e delle relative politiche e legislazione da implementare; gestisce denunce e conduce indagini; collabora con le amministrazioni nazionali dei paesi dell'UE per assicurare la coerenza legislativa nell'ambito della protezione dei dati; controlla le nuove tecnologie che possono influire sulla protezione dei dati.

---

[3] Che cos'è il reclamo e come si presenta al Garante, Garante per la protezione dei dati personali: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4535524

La privacy, questa sconosciuta

La libertà e segretezza della corrispondenza

La riservatezza e la segretezza della corrispondenza privata sono diritti umani tutelati a livello europeo (art. 7 e 8 Carta Diritti Fondamentali UE; art. 8 Convenzione Europea Diritti dell'Uomo; Regolamento Generale Protezione Dati UE 2016/679). L'art. 8 della Convenzione europea per i diritti dell'uomo, infatti, stabilisce che "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza".

La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali stabilisce, all'art. 10, che ogni persona ha "(...) libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera."

L'art. 15 della Costituzione italiana recita: "La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge." Questo significa che cittadini e stranieri, persone fisiche, giuridiche e formazioni sociali residenti sul suolo italiano sono tutelati nella riservatezza delle loro comunicazioni.

L'art. 15 della Costituzione, al secondo comma, contiene una doppia riserva, di legge e di giurisdizione, rendendo il giudice l'unico soggetto in grado di limitare la libertà di corrispondenza.

Per quanto concerne la riserva di legge, anch'essa è assoluta, per cui spetta ad una legge dello Stato stabilire con precisione i campi e le modalità di intervento giudiziario, in mancanza della quale spetta al giudice decidere sulla limitazione.

L'intercettazione è formalmente una limitazione della segretezza della corrispondenza. La Corte costituzionale è intervenuta sulla materia con la sentenza n. 34/1973, in cui stabiliva che il potere di intercettazione è riconosciuto al magistrato (e non alla polizia), previo controllo dell'effettiva necessità di ricorrere alla limitazione per reprimere gli illeciti penali (controllo di legittimità).

Inoltre, oltre alla motivazione, il giudice deve stabilire durata ed eventuale proroga dell'intercettazione.

Il Codice di procedura penale dedica una sezione alle intercettazioni di conversazioni o comunicazioni. L'art. 267, in particolare, stabilisce che l'autorizzazione è data con decreto motivato quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini.

Email e navigazione in Internet

Stati e governi non hanno la possibilità di intercettare tali comunicazioni senza l'intervento di un magistrato che garantisca il rispetto delle forme e dei requisiti di legge. Anche per "intercettare" il contenuto delle email per scopi di indagine, ad oggi, è ancora necessario l'intervento di un magistrato.

Al contrario, spesso i servizi di posta elettronica gratuita che utilizziamo (N.B. non i "client" come Outlook o Thunderbird ma i provider veri e propri quali Gmail, Yahoo, Hotmail, etc.) si riservano nel contratto la possibilità di effettuare una "scansione" automatica (quindi non una vera e propria lettura del senso e del significato del testo) dei termini contenuti nelle email che trasmettiamo, al fine di tracciare un profilo commerciale (e commerciabile) dell'utilizzatore.

Tale attività non risulta sempre conforme alle legislazioni dei diversi stati in materia di trattamento dati, tanto è vero che negli ultimi tempi molti provider

stanno cessando di propria iniziativa questo tipo di "lettura" del contenuto delle email. Anche la navigazione online è oggetto di screening e di attenzione da parte di istituzioni pubbliche e private.

Per quanto riguarda le istituzioni pubbliche, è bene sapere che in Italia la c.d. riforma Orlando (legge 103/2017) ha esteso la possibilità di utilizzare software di tipo trojan per monitorare navigazione e conversazioni degli utenti. Si tratta di un tema che, pur non suscitando vasto dibattito pubblico, ha raccolto molte critiche dagli addetti ai lavori. Al riguardo segnaliamo in particolare la dettagliata analisi di Privacy International, tradotta e condivisa da CILD.[4]

Inoltre, tutta la navigazione effettuata in internet è da sempre utilizzata a fini statistici e di profilazione utenti sia lato client (browser utilizzato) che lato server (siti web visitati e, in particolare, motori di ricerca).

Attraverso tecnologie più o meno raffinate come Cookies, Flash Cookies, Evercookies, Etags, HTML5 Web Storage, e Device Fingerprinting sia i siti web che i produttori di browser possono tracciare con un altissimo grado di precisione le attività e quindi i gusti degli utenti, al fine di comunicare pubblicità sempre più mirata ed ottenere un altissimo grado di personalizzazione del profilo utente.

Come proteggersi?

Innanzitutto, ogni browser può essere settato con l'opzione "Do-Not-Track" (DNT) attiva. Il DNT non è altro che una semplice richiesta inviata dal browser alle pagine web che comunica al server web la preferenza dell'utente riguardo alla raccolta dei suoi dati di navigazione, raccolta che viene utilizzata per esempio nel caso delle pubblicità personalizzate.

---

[4] Trojan di stato e i rischi della legge Orlando: serve dibattito pubblico CILD, 20 giugno 2017: https://cild.eu/blog/2017/06/20/trojan-di-stato-rischi-della-legge-orlando-sulla-sorveglianza/
Il testo originale dell'analisi di Privacy International è disponibile qui: https://www.documentcloud.org/documents/3728074-Privacy-International-s-Analysis-of-the-Italian.html

In realtà il DNT si è rivelato strumento scarsamente efficiente per eliminare completamente le attività di tracciamento sopra elencate. È però possibile rendere la navigazione meno tracciata con la controindicazione di renderla lenta e complessa.

Esistono oggi numerose estensioni per browser che consentono all'utente un maggior controllo sui propri dati di navigazione. Tuttavia, l'implementazione cumulativa di tutte le estensioni incide sulla qualità della navigazione rendendo molto lento il caricamento delle pagine. Inoltre, viene disattivata la possibilità di guardare video e, seppur raramente, anche il caricamento delle immagini può essere inibito. Le estensioni più conosciute e meglio funzionanti sono:

- AdBlock: serve a bloccare noiosi pop-up, banners e alcuni tracker;
- EFF Tracker Blocking Laboratory: simile ad AdBlock, funzionamento automatico tramite la generazione di una whitelist di siti che "sembrano" rispettare le richieste "Do-Not-Track" inviate dai browser;
- Ghostery: individua e consente il blocco di numerosi tipi di tracker;
- Lightbeam: non blocca i tracciatori ma ne consente il controllo attraverso la mappatura degli stessi. Attraverso delle visualizzazioni interattive, mostra i siti con cui, direttamente o indirettamente, l'utente interagisce mentre naviga;
- NoScript: (per utenti "avanzati") consente all'utente il diretto controllo sull'esecuzione di JavaScript, Java, Flash e altri plug-in su determinati siti ed il blocco su altri. Può seriamente inficiare la qualità della navigazione;
- Privacy Badger: controlla che non ci siano attività di tracking da parte di tracciatori di terze parti (cioè non direttamente collegati al sito che si sta visitando) bloccando automaticamente il caricamento dei contenuti collegati ai tracciatori;
- Https Everywhere: è un'estensione per Chrome, Opera e Firefox che, se installata, rende impossibile visualizzare siti che non siano disponibili con sistema di protocollo https. Quest'ultimo permette l'autenticazione del sito web visitato

sul server associato con cui si sta comunicando, proteggendo in questo modo dai cosiddetti man-in-the-middle attacks.

È bene ricordare che...

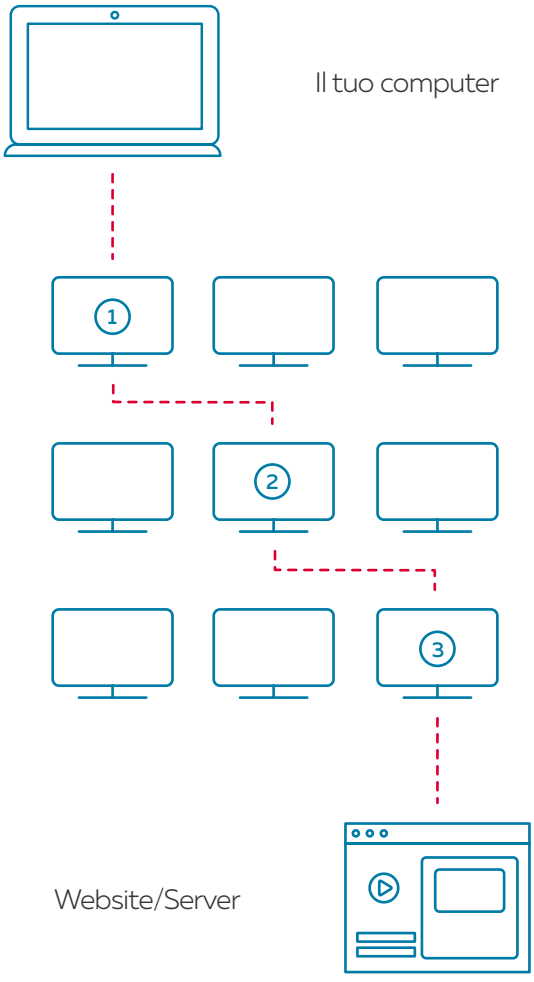
L'utilizzo di tali estensioni rende la diffusione delle proprie informazioni di navigazione a scopo di profilazione meno incontrollata. L'utilizzo quotidiano può essere utile per evitare la creazione di un preciso profilo di mercato dell'utente e per evitare casi di discriminazione dei prezzi in base alle proprie abitudini di navigazione e acquisto. Tuttavia, non protegge da attività di sorveglianza e controllo in senso stretto.

Per proteggere la propria navigazione e comunicazione da monitoraggio è possibile usare:

- PGP (Pretty Good Privacy) per quanto riguarda le comunicazioni: è un software di crittografia gratuito ma particolarmente avanzato che consente di cifrare comunicazioni tra utenti. Ad oggi, è comunemente considerato uno dei mezzi più sicuri per la trasmissione di informazioni confidenziali su internet.

- TOR (The Onion Router) per quanto riguarda la navigazione: è un sistema di navigazione anonima attraverso una rete di router che permettono il traffico anonimo in uscita. La controindicazione nell'utilizzo di TOR è esattamente la possibilità che il gestore di uno di questi nodi router sia un hacker malintenzionato o un ente di governo preposto al monitoraggio.

Come funziona Tor?



1 Punto di ingresso

2 Punto di transito

3 Punto di uscita

Connessione criptata

I dati vengono criptati all'interno del network ma mai nel punto d'uscita.

I punti di transito e di uscita cambiano casualmente ogni 10 minuti.

Tor devia la navigazione su almeno tre server prima di raggiungere la destinazione.

Il tuo IP e posizione rimangono nascoste per tutto il tempo della navigazione.

È anche possibile navigare attraverso l'utilizzo di una VPN (Virtual Private Network) canalizzando i propri dati di navigazione (come, ad esempio, indirizzo IP, indirizzi IP dei siti visitati, servizi utilizzati durante la navigazione, etc.) attraverso la rete virtuale schermando in questo modo il dispositivo utilizzato.

Tuttavia è da notare che, anche in questo caso, non tutti i provider di reti VPN sono trasparenti per quanto riguarda i dati dell'utente che transitano attraverso i loro canali. Generalmente, i servizi a pagamento non conservano e non trattano i dati di navigazione se non quando indispensabile a garantire il servizio. Diffidare di quelli gratuiti.

Infine, per quanto riguarda i motori di ricerca, è necessario ricordare che il core business di un fornitore di servizio di ricerca è esattamente quello di raccogliere le c.d. "queries" ovvero le ricerche, in modo da avere una idea sempre più precisa di "cosa" cerca il pubblico, collegandolo al "quando", "come" e "perchè", ossia a determinati momenti storici, luoghi geografici, motivazioni.

Tutto ciò avviene per ottenere un altissimo livello di profilazione dell'utente individuale e, soprattutto, di gruppi di utenti categorizzati e viene sostanzialmente utilizzato per creare pubblicità mirate, sviluppando ritorni economici.

In alternativa, è possibile utilizzare dei motori di ricerca alternativi e, ad oggi, ancora poco conosciuti (e, quindi, sicuramente meno efficienti nel ritorno dei risultati di ricerca rispetto ai concorrenti più accreditati) chiamati DuckDuckGo e Startpage.

Entrambi non collezionano i dati dell'utente e non condividono con terzi i risultati delle ricerche. La loro mission è esattamente quella di consentire l'utilizzo del servizio basilare di motore di ricerca senza compromettere la privacy degli utenti. È consigliabile utilizzarli quando si effettuano ricerche in merito ad informazioni sensibili, come, ad esempio, lo stato di salute relativo a se stessi.

È però opportuno ricordare che ottenere le informazioni che si cercano potrebbe essere più laborioso e meno immediato rispetto all'utilizzo di altri servizi.

Per un utilizzo consapevole dei social network

I social network 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 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. I social network 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.

Inoltre, in molti social network è permesso solo di "disattivare" il proprio profilo personale, senza possibilità di "cancellarlo", anche in caso di terminazione del servizio. I dati e le informazioni caricate online nel corso dell'utilizzo, sono comunque conservate nei server e negli archivi informatici dell'azienda che offre il servizio.

È bene ricordare che...

I social network non offrono servizi a titolo gratuito agli utenti, contrariamente a quanto si crede comunemente. Essi trovano la controprestazione ("causa") economica nel rapporto con l'utente attraverso l'apprensione ed il trattamento dei dati degli iscritti.

Una volta inseriti dati/informazioni su un sito di social network, se ne perde sostanzialmente il controllo. I dati possono essere registrati da tutti i contatti e dai componenti dei gruppi dei quali si fa parte. Possono essere conservati, rielaborati, diffusi, anche a distanza di anni. Quasi sempre, accettando di entrare in un social network, si concede all'impresa che gestisce il servizio la licenza di utilizzare senza limiti di tempo il materiale caricato online, come foto, chat, pensieri e,

eventualmente, anche su materiale protetto da copyright, quali ad esempio opere intellettuali (testi, canzoni, fotografie, etc.) prodotti dall'utente.

Le nuove norme europee in materia di trattamento dati stanno obbligando i fornitori di servizi ad offrire delle informative agli utenti semplici da capire. È bene abituarsi a leggere cosa esattamente prevedono termini e condizioni d'uso e le garanzie di privacy offerte nel contratto che si accetta al momento di una iscrizione ad un social network.

Il diritto all'oblio

Con il termine diritto all'oblio s'intende il "giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata".[5] Si fa riferimento, in particolare, al diritto di un individuo a non vedere distorta la propria immagine attuale a causa di una nuova diffusione di informazioni relative a vicende o affermazioni che in passato l'hanno visto protagonista, ma che non corrispondono più a quella che è l'attuale proiezione della propria identità all'interno della società.

Tale diritto è oggi espressamente riconosciuto e tutelato dal nuovo Regolamento per la Protezione dei Dati Personali n. 2016/679, secondo il quale sulla base di tali premesse è stato regolamentato il diritto alla cancellazione, o "diritto all'oblio". Al comma I, il principio stabilisce che "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali", quando ricorrono i motivi previsti dalla legge:

a. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

[5] Cass., sez. III, 9 aprile 1998, n. 3679, in Foro it., 1998, I, p. 1834

b. l'interessato revoca il consenso su cui si basa il trattamento;

c. l'interessato si oppone al trattamento ai sensi dell'articolo 1, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

d. i dati personali sono stati trattati illecitamente;

e. i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

I dati nel Cloud

Con il termine cloud computing, o semplicemente cloud, ci si riferisce a un insieme di tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo di software che rende possibile conservare ed elaborare grandi quantità di informazioni via Internet.

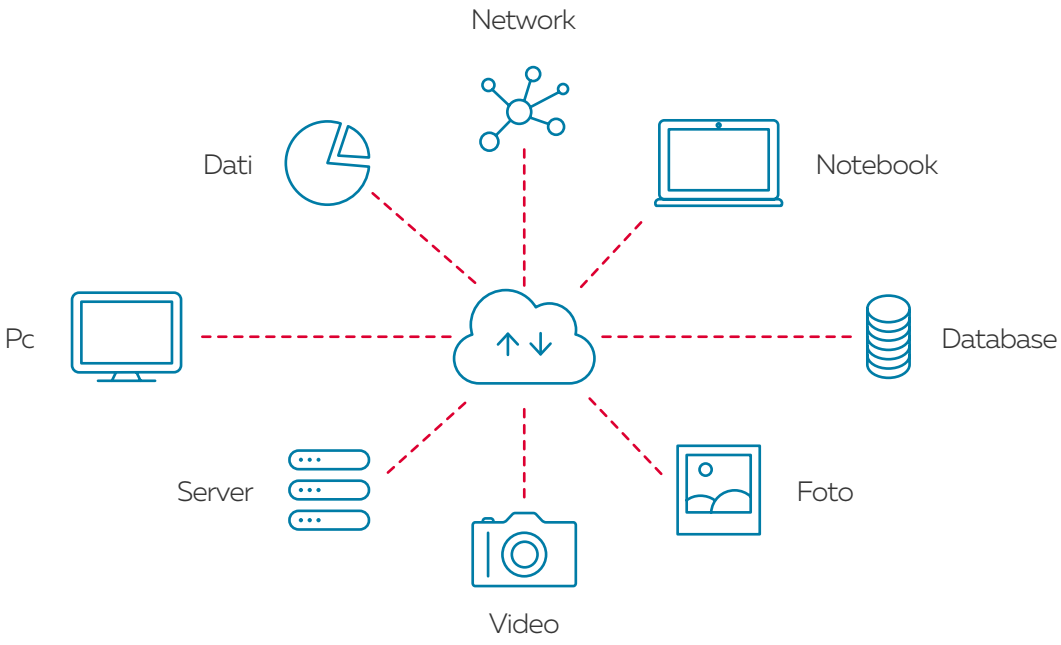
Il cloud offre, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai computer degli utenti ai sistemi del fornitore. Il cloud consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di computer e altri hardware avanzati, né di personale in grado di programmare o gestire un sistema di archiviazione dati. Solitamente il fornitore di servizi cloud dispone di sistemi di protezione contro virus, attacchi hacker o altri pericoli informatici più efficaci (e costosi) rispetto a quelli che potrebbero permettersi il singolo utente o la piccola azienda, rendendolo una scelta ovvia per lo svolgimento di attività economiche.

È comunque sempre necessario informarsi bene su quali siano le condizioni applicate dal cloud provider. Innanzitutto i servizi offerti "gratuitamente" quasi sempre prevedono attività di monitoraggio e controllo sui contenuti degli utenti.

Inoltre, si deve sempre considerare che, affidandosi a un fornitore remoto, esiste il rischio concreto relativo alla perdita di controllo diretto ed esclusivo sui propri dati.

Tra i tanti aspetti problematici nell'utilizzo dei servizi di cloud, alcuni meritano maggiore attenzione. Ad esempio per quanto riguarda i dati condivisi, è rilevante comprendere se il provider al quale li affidiamo, una volta sciolto il contratto con l'utente, cancelli o meno tutti dati. Per ora è pressoché impossibile verificare o escludere questa dinamica poiché potenzialmente i backup di ogni utente sono mischiati fra loro, rendendo particolarmente difficoltosa una cancellazione selettiva. Proprio per questo motivo quando accediamo a Gmail da un nuovo dispositivo ritroviamo tutte le email ricevute fino a quel momento. Inoltre, risulta ancora non troppo chiara l'attribuzione di responsabilità in materia di sicurezza: questa ora è divisa tra provider e cliente (a seconda del modello di cloud computing utilizzato, IaaS o SaaS), con il potenziale rischio che alcuni dati possano risultare scoperti da qualsiasi garanzia.

Quali sono i collegamenti al Cloud?



Violazioni comuni della normativa sul trattamento dati

Di seguito analizziamo alcune delle violazioni più comuni della normativa sul trattamento dei dati personali, con particolare riferimento al Codice della Privacy (artt. 18, 19, 23, 123, 126, 130 e da 167 al 172).

Spamming

Spamming o spam è l'invio, massiccio e ripetuto, tramite operatore o con modalità automatizzate, di comunicazioni non richieste (via telefono, e-mail, fax, sms, etc.), senza che il destinatario abbia ricevuto un'informativa sul trattamento dei dati personali o abbia prestato il consenso a ricevere messaggi. Come sempre nel caso dei dati, una buona educazione alla diffusione degli stessi è in grado di prevenire attività di spamming. In particolare è utile:

- non diffondere online indirizzi email o numeri di telefono qualora non sia strettamente necessario;
- leggere le condizioni del servizio e le informative privacy di tutti i servizi che richiedono il conferimento di un indirizzo email;
- controllare le impostazioni di visibilità del profilo sui social network, limitando l'accesso alle informazioni di contatto.

Nei casi di reiterazioni di attività di spamming subita dall'utente è possibile presentare segnalazioni, reclami e ricorsi al Garante per la protezione dei dati personali ovvero rivolgersi al giudice ordinario per l'eventuale risarcimento del danno nel caso il danneggiato sia una persona fisica.

Recupero crediti telefonico

Ogni attività di recupero crediti deve avvenire nel rispetto della dignità personale del debitore, evitando comportamenti che ne possano ledere la riservatezza a causa di un momento di difficoltà economica o di una dimenticanza.

Tuttavia nella prassi esistono casistiche di tentativi di recupero crediti svolti secondo forme invasive (visite a domicilio o sul posto di lavoro, reiterate sollecitazioni al telefono fisso o sul cellulare, telefonate preregistrate, invio di posta con l'indicazione all'esterno della scritta "recupero crediti", etc).

Per questo motivo, già dal 2005 esiste un provvedimento ufficiale del Garante[6] che prescrive a quanti svolgono l'attività di recupero crediti le misure necessarie perché tutto si svolga nel rispetto dei principi di liceità, correttezza e pertinenza.Secondo il provvedimento, sono da ritenersi illecite le modalità invasive di ricerca, presa di contatto, sollecitazione quali, ad esempio:

- visite al domicilio o sul luogo di lavoro con comunicazione ingiustificata a soggetti terzi rispetto al debitore di informazioni relative alla condizione di inadempimento nella quale versa l'interessato;
- comunicazioni telefoniche di sollecito pre-registrate, poste in essere senza intervento di un operatore, perché con questa modalità persone diverse dal debitore possono venire a conoscenza di una sua eventuale condizione di inadempienza;
- utilizzo di cartoline postali o invio di plichi recanti all'esterno la scritta "recupero crediti" o formule simili che rendono visibile a persone estranee il contenuto della comunicazione;
- affissioni di avvisi di mora (o, comunque, di solleciti di pagamento) sulla porta

[6] Liceità, correttezza e pertinenza dell'attività di recupero crediti - 30 novembre 2005, Garante per la protezione dei dati personali: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1213644

dell'abitazione del debitore, potendo tali dati personali essere conosciuti da una serie indeterminata di soggetti nell'intervallo di tempo (talora prolungato) in cui l'avviso risulta visibile.

Phishing e clonazione ("furto") di identità

Il phishing è una tecnica utilizzata per indurre un soggetto a comunicare a terzi informazioni riservate relative alla propria persona quali, ad esempio, le proprie username e password, i codici di accesso dei dispositivi elettronici (come il PIN del cellulare), numeri di conto corrente, dati del bancomat e della carta di credito, ecc.

In genere, questo tipo di truffa si presenta all'utente sotto forma di messaggi e-mail che, per vari motivi, invitano a fornire direttamente i propri dati personali, oppure a cliccare su un link che rimanda ad una pagina web dove è presente un form da compilare. I dati così carpiti possono poi essere utilizzati per fare acquisti a spese della vittima, prelevare denaro dal suo conto o addirittura per compiere attività illecite utilizzando il suo nome e le sue credenziali.

Il «ladro di identità» si presenta, in genere, come un soggetto autorevole (banca, gestore di carte di credito, ente pubblico, ecc.) che invita a fornire dati personali per risolvere particolari problemi tecnici con il conto bancario o con la carta di credito, per accettare cambiamenti contrattuali o offerte promozionali. Dati, codici di accesso e password personali non dovrebbero mai essere comunicati a sconosciuti.

È bene ricordare che...

In generale, banche, enti pubblici, aziende e grandi catene di vendita non richiedono mai informazioni personali attraverso e-mail, sms, social media o chat.

Se si ricevono messaggi sospetti, è bene non cliccare sui link in essi contenuti e non aprire eventuali allegati, che potrebbero contenere virus o trojan horse capaci di prendere il controllo di pc e smartphone.

Il phishing è una tecnica, tra le altre, che può essere utilizzata per compiere un reato più articolato e pericoloso quale il c.d. "furto di identità" (ID theft). Pur non

corrispondendo "materialmente" ad una sostituzione della persona, il furto di identità in rete viene ricondotto dalla giurisprudenza nell'ambito del reato di cui all'art. 494 c.p., relativo alla "sostituzione di persona" e art. 640-ter c.p. in materia di frode informatica. Il "furto" di identità si manifesta solitamente sotto varie forme di frode.

Le più conosciute sono:

- Financial Identity Theft: furto dell'identità "finanziaria" allo scopo di utilizzare i dati identificativi di un individuo o di un'impresa per ottenere denaro (90% dei casi) a danno della vittima;
- Criminal Identity Theft: uso dei dati della vittima per compiere atti illeciti di varia natura;
- Ghosting: costruzione di una nuova identità, diversa da quella originaria, appropriandosi dei dati di una persona defunta per varie finalità.

Inoltre il furto di identità è spesso usato nelle attività di "cyberbullismo": l'impersonificazione di un'altra persona è un mezzo per carpire informazioni e foto, che poi vengono usate per inviare messaggi solitamente diffamatori.

Chi ci guarda? Note sulla videosorveglianza

Oggi la videosorveglianza è particolarmente diffusa anche in considerazione dei bassi costi di implementazione di sistemi di controllo video rispetto al passato. Autorità istituzionali e soggetti privati ne fanno ormai abbondante uso.

Questo tipo di attività è severamente normato dalle attuali leggi in materia di trattamento dati in generale, e da alcuni provvedimenti del Garante italiano[7], in particolare.

Da tali norme discende che chi svolge attività di videosorveglianza deve quindi osservare quantomeno delle cautele minime, rispettando comunque il principio di proporzionalità tra mezzi impiegati e fini perseguiti.

Tali cautele possono essere così riassunte:

1. Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificare la conformità del trattamento delle immagini alle disposizioni indicate dalle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni;

[7] Provvedimento in materia di videosorveglianza - 8 aprile 2010, Garante per la protezione dei dati personali: http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680

2. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi;

3. Nei casi in cui la legge impone la notifica al Garante dei trattamenti di dati personali effettuati da determinati soggetti, questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza;

4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili;

5. Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo;

6. Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili - immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa;

7. Occorre determinare con precisione il periodo di eventuale conservazione delle immagini (normalmente da 24 ore al massimo di una settimana), prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorità giudiziarie o di polizia, che giustifica un allungamento dei termini di conservazione;

8. Occorre designare per iscritto i soggetti che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso di altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia;

9. I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi dei comportamenti di consumo), salvo le esigenze di polizia o di giustizia, e non possono essere diffusi o comunicati a terzi;

10. Per gli impianti di videosorveglianza finalizzati esclusivamente alla sicurezza individuale (ad esempio, il controllo dell'accesso alla propria abitazione) occorre che le riprese siano strettamente limitate allo spazio antistante tali accessi, senza forme di videosorveglianza su aree circostanti e senza limitazioni delle libertà altrui. Occorre inoltre che le informazioni raccolte non siano in alcun modo comunicate o diffuse.

Privacy in movimento: aereoporti, porti e valichi di confine

Nello specifico settore dei trasporti internazionali, dopo l'11 settembre 2001 si è assistito a una progressiva e costante compressione dei diritti legati alla privacy degli utenti.

Tale compressione sistematica ha finito con l'incidere anche sul c.d. accordo di Schengen sulla libera circolazione delle persone all'interno dell'Unione Europea che, dal 1995 (per l'Italia dal 1997) abolisce i controlli sistematici alle frontiere interne dei paesi aderenti all'area UE – restando sempre possibili controlli a campione – lasciando obbligatori i controlli per chi proviene dalle frontiere esterne. L'accordo non incide sui controlli all'interno di un Paese.

In generale, secondo le leggi vigenti in Europa, non è possibile opporsi a controlli / ispezioni sul bagaglio e sulla persona da parte delle autorità preposte. Gli Ufficiali e gli Agenti di polizia giudiziaria possono, infatti, procedere a ispezioni personali e perquisizioni, senza un mandato del giudice: se valutano ci sia fondata possibilità di trovare armi, esplosivi, munizioni o sostanze stupefacenti sulla persona o nel bagaglio (D.L. 306/1992 e D.P.R. 309/1990), tutte attività che rientrano normalmente nei controlli portuali, aeroportuali e dogane.

È bene ricordare che...

Quantomeno in Europa, è sempre possibile chiedere di essere controllati o avere i propri beni ispezionati in locale privato separato dal pubblico circostante.

Una negazione di tale richiesta, non giustificata da motivi di ordine pubblico, può comportare delle forme di risarcimento economico nelle sedi giudiziarie.

Nei controlli effettuati su treni in corsa e non in stazione, potrebbe non essere disponibile alcun locale separato per consentire l'ispezione privata. Anche in questo caso, opporsi al controllo potrebbe avere conseguenze più gravi quali, ad esempio, il fermo temporaneo presso gli uffici di polizia della prima stazione disponibile.

Fonti Normative

Carta dei Diritti Fondamentali della UE
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=LEGISSUM:l33501

Convenzione Europea dei Diritti dell'Uomo
http://www.echr.coe.int/Documents/Convention_ITA.pdf

Dichiarazione Universale dei Diritti dell'Uomo
http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf

Regolamento Generale sulla Protezione dei Dati 2016/679 (UE)
http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

Codice in Materia di Protezione dei Dati Personali (ITA)
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248

Convenzione di Schengen
http://eur-lex.europa.eu/summary/glossary/schengen_agreement.html?locale=it

Legge "Orlando" del 23 giugno 2017, n. 103 contenente modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario
http://www.gazzettaufficiale.it/eli/id/2017/07/4/17G00116/sg

Giurisprudenza Essenziale

- "Internet Usage Surveillance on the Workplace / Sorveglianza dell'utilizzo di internet sul posto di lavoro": ECHR 61496/08 "Brbulescu v. Romania" 05.09.2017
- "Right to be Forgotten / Diritto all'Oblio": CGUE C-131/12 "Google Spain" 13.05.2014
- "Data Retention / Tempi di Conservazione dei Dati": CGUE cause riunite C-203/15 e C-698/15 "Tele2 Sverige" 21.12.2016
- "Employee's Email Surveillance / Sorveglianza delle Email di un dipendente": ECHR 29107/95 "Stedman v. United Kingdom" 9.04.1997
- "Secrecy of Correspondence / Segretezza della Corrispondenza": ECHR Golden vs UK, 21.02.1975; Klass and Others vs Germany, 6.09.1978; Campbell and Fell vs UK, 28.06.1984; Silver vs UK, 25.03.1983; Malone vs UK, 2.08.1984; Leander vs Sweden, 26.03.1987; Kruslin vs France, 24.04.1990; Messina vs Italy, 26.02.1996; S. and Marper vs UK, 4.12.2008.
- "Utilizzo dell'immagine di una persona senza il suo consenso": Supreme Court of Georgia "Pavesich" 3.03.1905

Glossario

GDPR (general data protection regulation)

È il nuovo Regolamento UE n. 2016/679 che sostituisce la precedente Direttiva n. 95/46 CE e con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali all'interno dei confini dell'Unione europea. Il testo inizierà ad avere efficacia il 25 maggio 2018.

VPN (virtual private network)

La VPN è una rete privata creata per garantire sicurezza e anonimato della navigazione online attraverso protocolli di cifratura. Semplificando al massimo, una VPN crea un "tunnel virtuale" tra il nostro computer e un server sicuro di proprietà del fornitore del servizio VPN. Tutto il traffico che effettuiamo passa in modo criptato dal computer al server, per poi uscirne.

In dettaglio, una VPN è composta da due parti: una interna (generalmente più sicura) e una esterna (generalmente meno sicura) utilizzata per interconnettere tra loro i vari nodi della rete. Come funziona e come vengono garantiti i livelli di sicurezza in una VPN? Attraverso un meccanismo a tre livelli: un sistema di autenticazione, che permette l'accesso alla VPN solamente a utenti registrati, un metodo di cifratura, che consente di schermare i dati scambiati tra i vari nodi della rete; un firewall, che filtra gli accessi alle porte della rete. La cifratura è affidata a protocolli come l'IPsec, il Transport Layer Security (TLS/SSL), PPTP e il Secure Shell (SSH).

Le reti VPN si dividono tra reti ad accesso remoto, che connettono un individuo a un network, e reti *site-to-site*, che consentono la connessione tra due network differenti. La prima tipologia dà l'opportunità a un dipendente "fuori sede" o in telelavoro di connettersi all'intranet della propria azienda o ai documenti che condivide con gli altri colleghi; la seconda, invece, permette a differenti sedi di una stessa azienda o società di condividere una rete virtuale.

WP art. 29 (working party art. 29)

Comunemente noto come WP29, il Gruppo prende il suo nome in quanto istituito dall'art. 29 della direttiva 95/46. È un organismo consultivo e indipendente,

composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione Europea.

Fra i compiti più rilevanti:

- esaminare le questioni attinenti all'applicazione delle norme nazionali di attuazione della direttiva;
- formulare pareri sul livello di tutela nella Comunità e nei paesi terzi;
- consigliare la Commissione in merito ad ogni progetto di modifica della direttiva, di misure addizionali, o specifiche da prendere ai fini della tutela dei diritti e delle libertà, nonché in merito a qualsiasi altro progetto di misure comunitarie che incidano su tali diritti e libertà;
- formulare pareri sui codici di condotta elaborati a livello comunitario;
- formulare di propria iniziativa raccomandazioni su qualsiasi questione riguardi la protezione dei dati personali nell'Unione;
- definire i criteri di adeguatezza per i paesi terzi.

Il nuovo regolamento europeo sostituisce al WP29 l'EDPS (European Data Protection Supervisor) sostanzialmente con gli stessi compiti.

PROTEGGI I TUOI DATI PERSONALI

Guida pratica per saperne di più

REALIZZATO DA

CILD

CILD - COALIZIONE ITALIANA LIBERTÀ E DIRITTI CIVILI
via Monti di Pietralata, 16 – 00157 ROME - cild.eu - info@cild.eu