

Il termine inglese privacy indica la sfera privata degli individui, e quindi fa riferimento all’insieme di informazioni personali che non vogliamo diventino di dominio pubblico senza il nostro consenso. La tutela della privacy ha acquistato un’importanza centrale con la diffusione delle tecnologie della comunicazione e con la nascita di banche dati (i server) in cui sono raccolte informazioni personali di tutti i tipi.. La sfera privata diventa sempre più fragile, esposta a mille insidie. Da ciò nasce la necessità di allargare le frontiere del diritto alla TUTELA della RISERVATEZZA al di là delle informazioni riguardanti la sfera intima della persona.

In Italia la tutela della Privacy risiede oggi nel **Decreto n.101/18** **del 10 agosto 2018**, che ha ufficialmente recepito l’ormai famoso GDPR (acronico di General Data Protection Regulation) portando la tutela in materia di privacy QUASI uniforme in tutta l’UE.

**Il decreto 101 cosa fa:**



* Stabilisce cosa si intenda per:

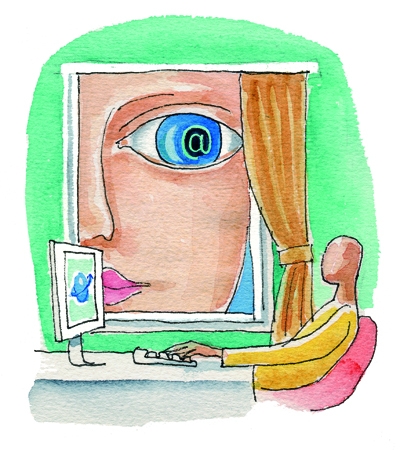
dato personale, ovvero delle informazioni relative a **persona fisica (cioè al singolo utente)** identificata o identificabile. La persona può essere identificata direttamente o indirettamente, grazie ad un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online (nick name o nome profilo) o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; così sono dati personali i DATI IDENTIFICATIVI (fotografie, video e qualsiasi cosa permetta l’identificazione diretta dell’interessato), i DATI ANAGRAFICI (nome e cognome, indirizzo mail, indirizzo di residenza e/o domicilio, numero di telefono, ecc.), i DATI FINANZIARI (codice fiscale, conto corrente, numero carta di credito, ecc.)

1. Dati personali particolari (o sensibili secondo il [codice privacy italiano](https://it.wikipedia.org/wiki/Codice_in_materia_di_protezione_dei_dati_personali))  come l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla vita sessuale o all'orientamento sessuale della persona, dati genetici, dati biometrici (come l’immagine facciale, grazie ai quali è possibile identificare una ed una sola persona fisica), dati sulla salute, informazioni su servizi di assistenza sanitaria (vedasi nel caso dell’APP IMMUNI nel caso della pandemia da COVID 19), dati personali relativi a condanne penali o reati.

* Stabilisce una disciplina per tutelare la riservatezza di queste informazioni, andando ad evitare che queste informazioni vengano acquisite (in modo lecito o illecito) e trattate da soggetti terzi in violazione a quanto previsto dal codice di tutela.
* Pretende, all’interno delle aziende (pubbliche e private che siano) la nomina di soggetti ( i DPO. Data Privacy Officer) che abbiano il compito e la responsabilità di verificare che il trattamento dei dati che gli utenti condividono con la società stessa siano raccolti e trattati in modo conforme alle previsioni del decreto.
* Prevede come necessario il consenso dell’interessato per il trattamento dei dati (qui sarebbe interessante capire quanti tra i ragazzi sanno a cosa stanno dando il consenso qualndo cliccano sul bottone “acconsento” accedendo ad un sito o ad una app) ☺
* Prevede una serie di sanzioni nel caso di mancato rispetto delle previsioni normative e, quindi di trattamenti illeciti.
* Stabilisce chi contattare e cosa fare nel caso si venga a conoscenza che un proprio dato è stato trattato in maniera illecita.

La privacy oggi è quanto mai importante ed ha acquisito sempre più importanza nella nostra società con l’esplosione dei social media. In effetti è sempre stato importante salvaguardare i dati personali delle persone, per evitare che questi venissero diffusi o comunicati a persone terze senza il consenso dell’interessato o tenuti in archivi accessibili a tutti, senza particolari cautele. Tuttavia la nascita e la diffusione dei internet prima, dello scambio di dati tramite i server ed infine, come dicevamo, la nascita e lo sviluppo dei social media e di tutte le piattaforme per l’E- commerce, le banche online, le mail e tutto il mondo digitale ha messo in luce l’importanza ma anche la pericolosità del trattamento senza cautele ed ha pertanto fatto si che i Garanti europei si siano attivati, nel corso degli anni per emanare norme che tutelassero i dati personali e sensibili degli utenti. Le normative, prima nazionali e disomogenee tra loro, oggi sono state uniformate a livello EU con il predetto GDPR.

Anche se non ce ne accorgiamo, tramite Internet diffondiamo e DIAMO IL CONSENSO a Società DI OGNI GENERE E Nazionalità, di trattare i nostri dati personali e sensibili. Internet ci osserva, e grazie al nostro consenso, sa tutto o quasi di noi (nome, cognome, dati genetici quali l’aspetto fisico, età, dati della carta di credito, dati sanitari, ma, ancora più pericoloso opinioni politiche, sociali, religiose e di ogni altro genere che condividiamo sui social quando pensiamo di star solamente commentando un post o scrivendo cosa stiamo facendo al nostro gruppo di amici. Tutti i dati che condividiamo vengono registrati e trattati, per finalità commerciali, di marketing, di PROFILAZIONE (cioè viene effettuato un profilo di chi siamo sulla base delle nostre caratteristiche e scelte manifestate, esplicitamente o implicitamente) da società di ogni nazionalità (se andate a guardare quando vi chiedono il consenso per i famosi cookies per poter accedere ad un qualsiasi sito scoprirete che i vostri dati vengono trasmessi, comunicati o diffusi), CON IL VOSTRO CONSENSO CHE ESPRIMETE SEMPLICEMENTE CLICCANDO UN BOTTONE CON SCRITTO ACCONSENTO con centinaia di società.



Questo per dare un’idea di quanto pericoloso sia immettere i propri dati personali (comprese le proprie opinioni personali su certi temi) in internet, dando il consenso al loro trattamento. Quindi società terze, a volte anche governative, sapranno quanti anni abbiamo, a che classe sociale apparteniamo in base al nostro titolo di studio, ai nostri acquisti, qual è la nostra opinione politica, chi sono i nostri amici etc.

Tutto questo ha, come sempre, un duplice profilo:

se da un lato, tutto questo “ Grande Fratello” ha permesso di fare un enorme passo in avanti in molti settori (si pensi a quello delle indagini, piuttosto che alla velocizzazione dei rapporti commerciali, potendo fare acquisti tramite internet anche in Cina senza bisogno di recarvisi) ed ha permesso di salvaguardare vite umane ( si pensi, in questo caso alle app per la geolocalizzazione che spesso rintracciano persone scomparse o alla attuale necessità di profilazione che il Governo sta mettendo in atto con la famosa App IMMUNI per il tracciamento dei profili affetti da covid e i relativi spostamenti) dall’altro lato è facile immaginare quanto pericoloso sia lasciare che degli sconosciuti vedano chi siamo e trattino i nostri dati per ogni tipo di scopo. E fino a qui abbiamo parlato degli scopi leciti.

Purtroppo internet lascia aperte molte porte anche all’utilizzo dei dati in modo illecito (ed è proprio per questo che è nato il GDPR, per vigilare). Sono sempre più frequenti infatti furti di identità, utilizzo delle opinioni espresse per scopi propagandistici (si pensi allo scandalo che scosse Facebook per la cessione dei dati degli utenti alla società Cambridge analitycs durante le elezioni USA), episodi di cyberbullismo, pornografia in rete e adescamento perché capita che dei filmati o delle foto condivise in rete vengano riutilizzate in maniera impropria. Ricordiamoci poi che tutto quello che viene condiviso su un social non può più essere cancellato, e resta in rete anche se viene cancellato il post o la foto quel dato resta comunque in archivio e potrebbe essere riutilizzato o analizzato.



Pensate che oggi tutto questo potrebbe, apparentemente non spaventarvi perché viviamo in uno stato di democrazia, ma immaginate cosa succederebbe se questi dati venissero esaminati durante una guerra, o in un momento politico diverso. Esistono delle regole pertanto, che devono essere condivise, soprattutto con i giovani, per far loro capire che la privacy e la riservatezza della propria vita personale, dei propri dati e della propria sfera di vita privata è importante e va tutelata, da noi stessi in primis. I giovani devono essere consapevoli che le proprie azioni in rete possono produrre effetti negativi anche nella vita reale e per un tempo indefinito.

Cosa succede se i nostri dati vengono violati o vengono trattati in maniera impropria (penso all’esempio delle email di phishing per rubare dati personali agli utenti)? In caso di violazione della privacy - come ad esempio la diffusione sul sito internet dei dati personali in assenza di una idonea base normativa, oppure il trattamento dei dati senza aver ricevuto una adeguata informativa o senza aver espresso uno specifico e libero consenso, qualora previsto - la persona interessata ( l’utente) può presentare una direttamente al Garante un’apposita segnalazione gratuita o un “reclamo” .

Il “ricorso”, invece, è riservato al caso in cui il titolare del trattamento non abbia dato adeguato riscontro alla richiesta dell’interessato di esercitare i propri diritti (accesso ai dati personali, aggiornamento, rettifica, opposizione) assicurati dal Codice della privacy. In alternativa al ricorso presentato al Garante, la persona interessata può rivolgersi all’autorità giudiziaria ordinaria. Ricordiamoci però che, al di là dell’azione giudiziaria, potremmo avere conseguenze serie e gravi sulla nostra vita privata o sulla nostra reputazione, anche in futuro.



Ecco allora una serie di regole da rispettare:

1. Ciò CHE CONDIVIDI RESTERà VISIBILE PER SEMPRE (questo potrebbe crearti problemi anche in futuro ad esempio per la selezione ad un colloquio)
2. Tutto ciò che condividi ha delle conseguenze, positive o negative
3. Condividi solo cose vere, non bugie o fake news (per le quali ora è previsto anche un reato)
4. Cerca di condividere cose utili e non solo inutili selfie per ottenere likes che non porteranno a nulla nella vita
5. Condividi ciò che ti rappresenta (un hobby, una passione, una filosofia di vita)- cerca di non dare un’idea sbagliata di te.
6. FAI ATTENZIONE: tutto ciò che condividi ti profila!
7. Ciò che condividi, come detto sopra, potrebbe farti correre dei rischi (pensiamo ad un video di terze persone girato in classe con dati sensibili di terzi soggetti..)
8. Ricorda tutto quello che condividi viene reso pubblico ed è quindi visibile a tutti e potenzialmente può essere rubato.

In conclusione, il diritto alla privacy allora deve essere inteso non solo come diritto di impedire ad altri la raccolta e la diffusione di dati personali, ma anche come diritto di controllare la raccolta, il trattamento e la divulgazione delle informazioni sul nostro conto: il diritto, cioè, di sapere se ci sono e quali sono le banche dati che contengono informazioni che ci riguardano, quale uso ne sarà fatto, a chi saranno comunicate e in che ambito verranno diffuse, nonché quello di accedere ai dati e farli correggere se scorretti o illeciti.

FATE ATTENZIONE A TUTTO QUELLO CHE FATE IN RETE E A CHI DATE IL CONSENSO AL TRATTAMENTO DEI VOSTRI DATI!