ARTICOLO DI ELEARNINGNEWS

Year 6 - number 202 Wednesday 11 may 2022

E-learning e privacy, come orientarsi nella Rete

Come proteggersi dagli attacchi degli hacker e dalla diffusione dei dati forniti sul web? Ecco le strategie che gestori di piattaforme e utenti possono seguire, per evitare di andare incontro a minacce per la privacy

Smart working, didattica a distanza e corsi online. L'**e-learning** e, in generale, le nuove tecnologie, sono entrate prepotentemente nella vita di tutti i giorni, interessando i vari aspetti della routine quotidiana. Dalla scuola, al lavoro e al tempo libero, sono sempre di più le persone che si rivolgono a piattaforme online, per accedere a corsi di formazione e aggiornamento, videoconferenze, riunioni da remoto, ma anche a giochi e musica. L'aumento dell'utilizzo di queste piattaforme e l'evoluzione delle nuove tecnologie porta con sé anche un altro aspetto: il rovescio della medaglia è rappresentato dalle minacce informatiche, che si fanno sempre più sofisticate e ingannevoli per gli utenti, esposti a potenziali rischi ogni volta diversi. Per questo motivo, l'attenzione alla **privacy** e alla protezione dei dati forniti sul web è diventata un aspetto fondamentale, di cui avere particolare cura, sia da parte di chi naviga in Rete, che da parte del responsabile del trattamento dei dati.

Per l'Italia, la principale figura di riferimento in questo ambito è rappresentata dal **Garante per la protezione dei dati personali**, l'autorità che ha il compito di tutelare i diritti e garantire il rispetto della dignità nel trattamento dei dati personali. La normativa di riferimento è il *Regolamento generale sulla protezione dei dati*, approvato dal Parlamento e dal Consiglio europeo nel 2016 e in vigore dal 23 maggio 2018.

Privacy: le regole

Il *Regolamento sulla protezione dei dati* (*General data protection regulation*, Gdpr) si riferisce al "trattamento interamente o parzialmente automatizzato di dati personali" e detta le regole per riuscire a districarsi nei meandri della Rete in ambito di protezione della privacy. Il documento precisa i casi in cui è opportuno procedere al trattamento dei dati personali. In particolare, perché ciò sia lecito deve ricorrere almeno una delle seguenti **condizioni**:

- L'interessato ha espresso il consenso al trattamento;
- Il trattamento è necessario per un contratto, come quelli di fornitura di servizi o gli abbonamenti;
- Il trattamento è necessario per un obbligo legale, come nel caso in cui debbano essere forniti i dati del lavoratore all'Inps;
- Il trattamento è necessario per salvaguardare gli interessi vitali della persona, per esempio per motivi di salute;
- Il trattamento è necessario per svolgere un compito di pubblico interesse o per l'esercizio di pubblici poteri, come nelle scuole o nella Pubblica Amministrazione;
- Il trattamento è giustificato dal legittimo interesse, come nel caso di verifiche bancarie.

La richiesta di **consenso** al trattamento dei dati personali deve essere presentata in modo "chiaramente distinguibile" e con una "forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro". Trasparenza e chiarezza sono quindi le caratteristiche fondamentali su cui deve puntare il titolare del trattamento, per fare in modo che l'interessato sia in grado di fornire il proprio consenso al trattamento dei dati in modo consapevole.

Una volta dato il consenso, però, l'utente può sempre ritirarlo. L'articolo 7 del Regolamento sul trattamento dei dati, infatti, ricorda che "l'interessato ha il diritto di **revocare** il proprio consenso in qualsiasi momento". Ma, anche nel caso in cui il consenso venga revocato, la liceità del trattamento non è pregiudicata.

I Cookie: cosa sono e a cosa servono

Solitamente, quando si naviga in Rete, all'apertura di una pagina web o di una piattaforma, una finestra avvisa della presenza di **Cookie**. Ma cosa sono e a cosa servono i Cookie? E perché sono importanti per la privacy? Si tratta di file, che i siti visitati dagli utenti inviano al dispositivo dal quale si sta navigando, il quale li memorizza e li ritrasmette agli stessi siti nel momento della visita successiva. I Cookie permettono di semplificare e velocizzare gli accessi ai siti web da parte degli utenti, perché

memorizzano informazioni al primo accesso, e sono in grado di semplificare la fruizione, tenendo traccia, per esempio, degli articoli precedentemente inseriti in un carrello online. Oltre a queste funzioni, i Cookie sono molto utili anche ai gestori dei siti, che li utilizzano per la raccolta e il trattamento dei dati personali, come indirizzo IP e indirizzo e-mail.

Lo scorso giugno, il Garante ha approvato nuove Linee guida in materia di Cookie e strumenti di tracciamento, in base alle quali i titolari del trattamento sono invitati a fornire agli utenti un'informativa trasparenze e accessibile. Per farlo, questa deve avere un **linguaggio semplice** ed essere dislocata su più livelli, per esempio con il ricorso a pop-up. Il Garante precisa che i Cookie possono essere sia tecnici, che non tecnici. Nel primo caso, l'informativa può essere inserita in home page, mentre nel secondo caso deve essere previsto l'utilizzo di un banner a comparsa e ben visibile, che contenga:

- Un comando per chiudere il banner;
- L'indicazione sull'uso dei Cookie;
- Il link alla privacy, contenente l'informativa completa;
- Un comando per accettare tutti i Cookie;
- Un comando o un link per poter scegliere i Cookie da accettare.

E-learning e privacy

Anche l'uso delle **piattaforme LMS**, destinate all'e-learning, implica il trattamento dei dati personali degli utenti. L'impiego di una piattaforma permette al titolare di collezionare diversi dati riguardanti le persone che accedono al corso, come data di nascita, indirizzo e-mail, numero di telefono, nome e cognome e il profilo con cui l'utente è registrato sui social. Per questo, è necessaria una maggiore attenzione al trattamento dei dati, sia da parte dai gestori di queste piattaforme, che da parte dell'utente.

Leggi anche **eLearning e GDPR**.

Il gestore deve assicurarsi di agire in modo conforme al *Regolamento sulla protezione dei dati*, fornendo un'**informativa** sulla privacy chiara, di facile comprensione e accessibile, e rendendo evidenti le condizioni d'uso del LMS in questione. Per tutelare la privacy degli utenti, il fornitore LMS non deve raccogliere più dati di quelli necessari per lo scopo, né utilizzarli per scopi diversi da quelli dichiarati. L'articolo 13 del Regolamento europeo stabilisce le informazioni che il titolare del trattamento è tenuto a fornire all'interessato, nel momento in cui richiede i dati. In generale (e quindi anche per il trattamento dei dati in una piattaforma e-learning), l'informativa deve contenere:

- Dati di contatto del titolare;
- Dati di contatto del responsabile della protezione dati;
- Le finalità del trattamento dei dati e la base giuridica del trattamento;
- Eventuali destinatari dei dati;
- L'eventuale intenzione del titolare al trasferimento dei dati a terzi.

Una volta ottenuti i dati, il titolare deve indicare anche il periodo di conservazione dei dati, l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati, la possibilità di revoca del consenso e il diritto di effettuare un reclamo all'autorità di controllo.

Per essere certo di agire in modo conforme al Regolamento, il gestore della piattaforma e il titolare dei dati possono ricorrere ai numerosi **corsi e-learning** sulla privacy, cioè corsi di formazione effettuati da remoto, con l'aiuto di una piattaforma LMS, in cui vengono spiegate le basi delle regole per la gestione dei dati personali.

Da una parte, quindi, il gestore deve fare in modo di assicurare il rispetto delle finalità e delle modalità di trattamento, ma dall'altra è bene che anche gli utenti adottino le strategie necessarie per proteggersi.

Come proteggersi?

Per garantire la **protezione della privacy** degli utenti, il gestore della piattaforma o del sito e il titolare devono attenersi alle linee guida sul trattamento dei dati. Ma cosa può fare il singolo utente per mantenere in sicurezza i propri dati? Per essere maggiormente certi di conservare al sicuro i propri dati, è possibile adottare le seguenti strategie:

1. Utilizzare software di sicurezza: per evitare che un hacker possa penetrare nei tuoi dispositivi, è bene installare

programmi antivirus, in grado di proteggere pc, smartphone e tablet. Perché la protezione sia efficace, però, non basta installare l'antivirus: è necessario mantenerlo aggiornato e pianificare scansioni regolari, che controllino l'eventuale presenza di minacce alla sicurezza sul dispositivo.
2. Utilizzare la **rete privata virtuale** (VPN), per nascondere l'indirizzo IP e crittografare il traffico internet.
3. Rendere privati i profili **social**, per evitare che persone sconosciute possano aver accesso ai tuoi dati e visualizzare i post o i luoghi in cui ti trovi.
4. Usare una **password** a prova di intrusi, che non permetta ad altri di accedere facilmente alle tue mail, i tuoi profili o ai tuoi dati.

Relativamente all'ultimo punto, il Garante per la protezione dei dati personali dà alcuni suggerimenti per guidare gli utenti nell'impostazione di una **password sicura** e a prova di privacy. Per raggiungere questo obiettivo, la password deve avere le seguenti caratteristiche:

- Essere lunga almeno otto caratteri;
- Contenere almeno quattro diverse tipologie di caratteri: lettere maiuscole, minuscole, numeri e caratteri speciali (come quelli di interpunzione);
- Non contenere riferimenti personali facili da indovinare, come il nome e il cognome;

Sarebbe utile anche impostare una password con parole di fantasia, dato che esistono software in grado di decifrare le parole di uso comune nelle varie lingue. Scegliere la parola chiave per mantenere al sicuro i propri dati, però, non basta. Sarebbe bene, infatti, aggiornare periodicamente la password e utilizzare meccanismi di autenticazione che richiedano la presenza di più fattori (come codici OTP o sms). Meglio variare le password che proteggono account diversi, non usare parole chiave già utilizzate in passato ed evitare di scriverla su biglietti o condividerla via mail o sms.