

# Safer Internet Day

Dal 2004 il 9 febbraio di ogni anno si celebra in Europa il **Safer Internet Day (SID)**, evento nato con il *Safer Internet Action Plan* che fu elaborato per il periodo 1999-2004.

Il piano aveva l'obiettivo di incoraggiare la creazione di un ambiente favorevole allo sviluppo dell'industria connessa ad Internet promuovendo l'uso sicuro di Internet e lottando contro i contenuti illegali e nocivi.

Il programma (1999) si articolava su tre piani:

- creazione di un ambiente più sicuro mediante l'istituzione di una rete europea di linee dirette (hotline), incoraggiamento dell'autoregolamentazione e dell'elaborazione di codici di condotta;
- sviluppo di sistemi di filtraggio e di classificazione;
- iniziative di sensibilizzazione.

Nel corso degli anni, l'Europa ha comunque continuato a promuovere iniziative (*Safer Internet Plus*) con la finalità di realizzare Internet come un luogo sicuro per i ragazzi.

Anche quest'anno, quindi, il 9 febbraio si celebra il Safer Internet Day 2021, giunto alla sua 18ma edizione, e il tema è "*Together for a better internet*" (insieme per un internet migliore).

L'iniziativa è gestita dai *Safer Internet Centres* esistenti in ciascuno Stato membro.

L'iniziativa è finanziata dall'Unione Europea e la giornata viene celebrata online in più di 170 paesi del mondo.

**Mariya Gabriel**, Commissario europeo per l'innovazione, la ricerca, la cultura, l'istruzione e la gioventù, ha dichiarato: *"I giovani hanno bisogno di sentirsi sicuri e responsabilizzati quando navigano nel mondo online per poter godere appieno del mondo digitale. Con il Piano d'azione europeo per l'alfabetizzazione digitale, mettiamo l'alfabetizzazione digitale al centro del panorama educativo europeo, promuovendo l'alfabetizzazione digitale per combattere la disinformazione online, sostenendo educatori e insegnanti e assicurando un e-learning di qualità"*.

Il Commissario europeo per il mercato interno **Thierry Breton** ha dichiarato: *"La crisi del coronavirus ci ha costretti a spostare la maggior parte delle nostre attività quotidiane online e quando lasciamo i nostri figli navigare in internet, vogliamo che siano protetti. Siamo determinati a garantire che la trasformazione digitale porti benefici a tutti in modo sicuro. Ciò che è illegale offline dovrebbe essere illegale online. Ora ci aspettiamo che l'industria tecnologica faccia la sua parte nel rendere internet più sicuro senza indugio e in linea con le regole dell'UE"*.

La Commissione europea con il **comunicato stampa dell'8/2/2021** precisa che la Direttiva sui servizi di media audiovisivi (Audiovisual Media Services Directive -

AVMSD) richiede alle piattaforme di condivisione video online di limitare l'accesso dei bambini a contenuti dannosi e le regole per le piattaforme digitali.

Inoltre, la legge sui servizi digitali e la legge sui mercati digitali, proposte nel dicembre 2020, includono obblighi specifici per le grandi piattaforme per affrontare rischi significativi per il benessere dei minori.

Il **Safer Internet Day**, comunque, è l'occasione per evidenziare quanto la protezione dei dati personali e la privacy siano importanti unitamente, ovviamente, agli aspetti di sicurezza informatica.

Le piattaforme digitali online, quali titolari del trattamento, sono obbligate al rispetto delle norme in materia di protezione dei dati personali e precisamente del Regolamento UE 2016/679 e del codice privacy italiano (D.Lgs. 196/2003, così come modificato dal D.lgs. 101/2018).

Per la Repubblica di San Marino la disciplina in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali è la L. 171/2018 che è in vigore dal 5/1/2019.

Tuttavia, quando si parla di minori non si può fare riferimento unicamente alle norme.

La famiglia è il nucleo primario della società e resta il principale contesto all'interno del quale i minori si relazionano con i propri genitori.

I genitori, da parte loro, esercitano la

responsabilità genitoriale sui figli minori e sono tenuti a svolgere il controllo sebbene senza una profonda interferenza sulla loro sfera personale.

Tale controllo dovrebbe essere esteso anche alle attività che i minori compiono online.

Del resto, ciò è espressamente indicato nel citato GDPR, ove si fa riferimento al consenso "prestato o autorizzato dal titolare della responsabilità genitoriale" sul minore di anni 13 (questa l'età minima per quanto riguarda l'offerta diretta di servizi della società dell'informazione, ma dipende dal singolo Paese; in Italia è fissata a 14 anni).

La questione può apparire semplice, ma in realtà non lo è affatto in quanto è molto difficile controllare l'età effettiva e, ancora di più, la vera identità di colui che chiede l'accesso ad una risorsa online.

Sarebbe necessario un intervento legislativo sulla identità digitale che - al di là dello SPID italiano - sia valida quanto meno a livello europeo e anche interoperabile tra gli Stati membri.

Sono allo studio alcune proposte sulla identità digitale, ma il problema, comunque, per i minorenni resta.

Il discorso è ampio e meriterebbe maggiori spazi di approfondimento.

Bisogna investire su campagne di informazione e sensibilizzazione per accrescere nei minori la consapevolezza del

valore che hanno dati personali.



Nicola Fabiano

---

# Data Protection Day 2021

Il 28 gennaio 2021, si è celebrata la 15ma Giornata della protezione dei dati personali - Data Protection Day.

Infatti, il 26 aprile 2006, il Comitato dei Ministri del Consiglio d'Europa ha deciso di lanciare una Giornata della protezione dei dati, da celebrare ogni anno il 28 gennaio.

La Convenzione 108 è stato il primo trattato internazionale vincolante sulla protezione dei dati e un modello per molti altri regolamenti sulla protezione dei dati.

Quest'anno, poi, si è celebrato anche il **40mo anniversario** della apertura alla firma della Convenzione 108 del Consiglio d'Europa per la protezione delle persone rispetto al trattamento automatizzato dei dati personali.

Infatti, il 28 gennaio 1981 a Strasburgo veniva aperto il Trattato n. 108 (riferimento è ETS No.108) del Consiglio d'Europa alla firma degli Stati membri e all'adesione degli Stati non membri.

Il titolo del Trattato n. 108 è "Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale".

**La Convenzione 108 (ETS n. 108) è entrata in vigore l'1 ottobre 1985 con 5 ratifiche.** L'Italia l'ha firmata il 2 febbraio

1983 e ratificata il 29 marzo 1997, ma la data dell'entrata in vigore è l'1 luglio 1997.

Questa Convenzione rappresenta il primo strumento internazionale obbligatorio che ha per scopo la protezione delle persone contro l'uso abusivo del trattamento automatizzato dei dati di carattere personale, e che disciplina il flusso transfrontaliero dei dati.

Oltre alle garanzie previste per il trattamento automatizzato dei dati di carattere personale, la citata Convenzione 108 bandisce il trattamento dei dati «delicati» sull'origine razziale, sulle opinioni politiche, la salute, la religione, la vita sessuale, le condanne penali, in assenza, di garanzie previste dal diritto interno.

**Il 18 maggio 2018**, dopo 7 anni di intenso lavoro e negoziati, viene adottato dalla 128a sessione ministeriale del Comitato dei Ministri del Consiglio d'Europa, tenutasi a Elsinore, in Danimarca il Protocollo (CETS n. 223) che modifica la Convenzione 108.

Essa, quindi, viene rinnovata in una versione modernizzata denominata Convenzione 108+.

**La Convenzione 108+ si compone di complessivi 31 articoli ed entrerà in vigore con la ratificazione da tutte le Parti del Trattato STE 108, oppure l'11 Ottobre 2023, se a tale data ci saranno 38 parti del Protocollo.**

Allo stato attuale risultano 10 ratifiche e 33 firme non seguite da ratifica. L'Italia l'ha firmata il 5 marzo 2019 e non ancora

ratificata; San Marino l'ha firmata il 16 luglio 2019 e non ancora ratificata.

Il mese di maggio del 2018 ha visto anche l'applicazione del Regolamento UE 2016/679, meglio noto come GDPR (acronimo di General Data Protection Regulation), che costituisce la disciplina europea sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Al citato regolamento, per l'Italia, si aggiunge la disciplina del codice privacy (D.Lgs. 196/2003).

A chi forniamo i nostri dati personali e perché?

È necessario acquisire consapevolezza.

Il salto di qualità può essere fatto unicamente con una consapevolezza adeguata al tema che affrontiamo o che ci proponiamo di affrontare.

Quali sono le sfide da affrontare?

Tra le principali sfide, va menzionata certamente la **pandemia da COVID-19**, i quali effetti sono sotto gli occhi di tutti: questa, tuttavia, non è solo valutabile da un punto di vista medico e sanitario e presenta diverse questioni legate proprio alla protezione dei dati personali.

Da un lato, è innegabile che dall'inizio della pandemia ci sia stato un incremento esponenziale dell'uso delle tecnologie e delle risorse digitali disponibili, ma si è parlato poco dei rischi collegati alla privacy e alla

protezione dei dati personali.

Dall'altro, il trattamento di grandi quantità di dati sulla salute delle persone fisiche va effettuato nel pieno rispetto della legislazione vigente e con l'adozione di tutte le opportune misure di sicurezza.

Inoltre, in questi ultimi tempi si parla molto di vaccini e il contesto internazionale si sta interrogando sulla liceità di soluzioni quali il vaccine passport o immunity passport.

Altra sfida è quella dell'**Intelligenza Artificiale** (AI).

La Commissione europea da tempo ha creato il gruppo di esperti denominato "AI High Level Group" e il CoE ha creato il Comitato ad hoc sulla Intelligenza Artificiale (CAHAI).

Inoltre, proprio il 28 gennaio il Consiglio d'Europa ha pubblicato le linee guida sul **riconoscimento facciale**, affermando la necessità di una regolamentazione rigorosa per prevenire le violazioni dei diritti umani.

Ulteriore sfida, come ho già detto in diverse occasioni e da ultimo nel mio libro, è quella relativa alle **Neuroscienze**.

In particolare, esiste un allarme legato all'impatto che le tecnologie adottate nell'ambito delle neuroscienze possono avere su protezione dei dati personali e privacy.

Si tratta di un aspetto che negli USA stanno osservando da tempo, ma - in ragione dell'approccio alla privacy di quel Paese - con

risultati aderenti al loro impianto costituzionale.

Questi fenomeni vanno valutati attentamente; senza dubbio l'etica è un elemento fondamentale.

Il mio approccio, basato sul modello relazionale denominato DAPPREMO (acronimo di Data Protection and Privacy Relationships Model), potrebbe essere utile per approfondire questi aspetti.

Il tema delle neuroscienze in relazione all'impatto su protezione dei dati personali e privacy, senza dubbio, potrebbe essere quello di maggiore importanza per i nostri tempi, tanto che - provocatoriamente - ho lanciato l'idea di una nuova categoria di diritti che ho definito "neuroprivacy rights".



# Nicola Fabiano

*Privacy e azienda: la chimera della non applicabilità.*

*Cyber Psicologo e la privacy*