LA PROTEZIONE DEI DATI PERSONALI DEL MINORE

WEBINAR DEL 19 GENNAIO 2021

"L'identità digitale del minore e l'esposizione agli algoritmi comportamentali. Quali tutele?"

Intervento a cura dell'Avv. Rosa De Caria, Componente Commissione "Privacy"

***

L'accesso al *Web* deve essere ritenuto un diritto fondamentale in quanto proiezione diretta delle libertà costituzionali già riconosciute e necessarie per il pieno sviluppo della personalità dell'individuo: libertà di manifestazione del pensiero, libertà di istruzione, di cultura, di religione.
Il web rappresenta un'opportunità ma, il suo rovescio è la scia informatica che ogni persona lascia inconsapevolmente nella rete, consentendo la costruzione di un'identità digitale analizzata, sistematicamente, dagli algoritmi dei motori di ricerca.

Ma cosa intendiamo esattamente quando parliamo di 'identità digitale e in che rapporto dobbiamo porla con l'identità personale?

L'ordinamento tutela il «patrimonio intellettuale, politico o sociale di ogni persona»; la sua violazione implica violazione del diritto all'identità personale, protetto dall'art. 2 Cost., e ciò anche in assenza di una lesione del diritto all'onore o alla dignità. L'identità personale è qualcosa di distinto sia dal nome, sia dalla reputazione, perché in essa, sono racchiuse in modo sintetico tutte le caratteristiche e tutte le manifestazioni del proprio essere di ciascun individuo.

L'identità digitale è qualcosa di diverso e di più ristretto rispetto all'identità personale, perché riguarda, oltre che la proiezione nel *Web* del patrimonio di idee e di azioni della persona, anche ulteriori aspetti che sono propri della dimensione informatica e dunque i dati biometrici, le abitudini di spostamento, di acquisto, le preferenze di lettura, le opinioni sociali e politiche, la reputazione.

L'identità digitale è un insieme di dati personali idonei a delineare una persona, non solo per quello che dice che fa fuori e dentro la rete, ma anche e soprattutto per la traccia informatica che lascia consapevolmente con la navigazione informatica ma, anche inconsapevolmente, mantenendo i propri *chip* attivi.

Il tema è quello della profilazione e dell'esposizione agli algoritmi comportamentali.

La navigazione in rete di ciascun individuo permette ai soggetti digitali di accumulare masse immense di dati; lo sfruttamento e la riutilizzazione di tali dati costruisce la "storia digitale" di ciascun individuo che diviene così obiettivo di pubblicità e

contenuti mirati, basati su specifiche caratteristiche, sugli interessi individuali, sulle preferenze facilmente individuabili attraverso il meccanismo dei like. Ad un certo punto, dunque, la storia digitale di ciascun individuo, diventa strumento per orientarlo nelle abitudini di vita, nelle scelte commerciali, nei gusti musicali, di lettura, nelle opinioni politiche e poi ad un certo punto anche per discriminarlo ovvero, in momenti di crisi democratica, per privarlo di parte dei suoi diritti inviolabili.

La questione assume contorni particolarmente inquietanti, se letta alla luce dei dati Istat di accesso alla rete da parte dei minori, dei c.d. "nativi digitali". Si tratta, infatti, di soggetti vulnerabili, più facilmente influenzabili e plasmabili dalla forza degli algoritmi comportamentali.

I dati Istat ci dicono che nel 2019 il 27,4 % dei bambini tra i 6 e i 10 anni ha utilizzato internet quotidianamente; la frequenza di utilizzo quotidiano sale al 68,3% nelle fasce 11-14 anni e arriva all' 83,7% nelle fasce 15-17 anni.

Tra le attività preferite in Rete spiccano quelle legate a giochi, musica, immagini e film, la consultazione di wikipedia e la partecipazione a un social network.

Secondo una ricerca realizzata dal consorzio MIUR Generazioni Connesse in collaborazione con alcune università italiane tra cui La Sapienza di Roma, su un campione di 5942 adolescenti tra gli 11 e i 19 anni intervistati nel gennaio 2019 è emerso che 7 giovani su 10 si sono iscritti ad un social network prima dei 14 anni.

Il 16° Rapporto Censis sulla comunicazione indica la preferenza dei giovanissimi per YouTube ed Instagram. Tik Tok con numeri elevatissimi ed un picco di download a fine 2020, risulta il fenomeno del momento, soprattutto tra i giovanissimi.

Di fronte ad un fenomeno di tale portata, ci si deve interrogare se il sistema normativo assicura a tali soggetti una protezione adeguata.

Un punto fondamentale di riferimento, deve essere individuato, innanzitutto, nel fondamentale diritto del fanciullo al rispetto della sua vita privata e familiare, che si traduce, nel diritto a non subire arbitrarie interferenze nella vita privata, nella famiglia, nel domicilio, nella corrispondenza e a non subire lesioni all'onore e alla reputazione, come sancito dall'art.16 della Convenzione Di New York Sui Diritti Dell'Infanzia e Dell'adolescenza del 1989. La Carta dei diritti fondamentali dell'Unione Europea all'art 24 paragrafo 2 prevede, poi, che, <<*in tutti gli atti relativi ai minori, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del minore deve essere sempre considerato*>>.

Questi i principi informatori anche della normativa in materia di protezione dei dati personali dei minori, oggi rappresentata dal Regolamento UE 2016/679 (c.d. "GDPR"), recepito in Italia dal D.Lgs. 101/2018.

Il Considerando 38 richiama, infatti, l'attenzione sulla necessità di apprestare una specifica protezione ai dati personali dei minori, perché si tratta di soggetti che possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate e meno consapevoli dei loro diritti in relazione al trattamento dei dati personali. "Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore".

Da questo principio discende il regime speciale dettato dall'art.8 GDPR, in tema di consenso al trattamento dei dati del minore, in forza del quale, limitatamente all'offerta diretta di servizi delle società dell'informazione ai minori, è prevista - quale condizione di liceità del trattamento, l'età minima di 16 anni, ovvero in mancanza del requisito dell'età, il consenso o l'autorizzazione da parte del titolare della responsabilità genitoriale». La norma – da leggere anche tenendo conto di quanto previsto dalle Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 adottate dall'allora *Article 29 Working* Party e di recente aggiornate dalle Linee guida 5/2020 sul consenso ai sensi del Regolamento 2016/679 dell'EDPB – ha lasciato un margine di intervento ai singoli Stati Membri per la definizione di un'età inferiore riconoscendo agli <<*Stati membri la possibilità di stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni*». Il legislatore italiano ha inserito nel Codice Privacy l'articolo 2-*quinquies*, fissando il limite minimo a quattordici anni. In Francia è stata prevista l'età minima di 15 anni, in Germania di 16 anni, in Spagna e in Austria di 14 anni come in Italia.

Il consenso al trattamento dei dati dei minori quale condizione di liceità- validità del trattamento dei dati personali, assume una particolare rilevanza, perché esprime una forma di garanzia tesa ad assicurare il c.d. "*best interest of the child*", in conformità con quanto già sancito all'art 24 par. 2 della Carta dei diritti fondamentali dell'UE. Altrettanto significativo appare il formale riconoscimento assegnato agli esercenti la responsabilità genitoriale, chiamati a prestare il consenso o ad autorizzare il trattamento dei dati dei figli che non abbiano l'età minima richiesta dal legislatore.

Elemento chiave del consenso è l'informazione: il GDPR richiede un consenso al trattamento dei dati personali libero, specifico, inequivocabile ed informato.

Con specifico riguardo a soggetti deboli come i minori, l'art 2 quinquies comma 2 D.Lgs 101/2018 recependo quanto stabilito all'art 12 GDPR (in attuazione del considerando 58) espressamente sancisce che l'informazione deve essere resa accessibile attraverso un linguaggio chiaro e semplice in modo che il minore possa capire facilmente.

Il titolare del trattamento ha, dunque, l'obbligo di redigere un prospetto informativo chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, contenente le informazioni e le comunicazioni inerenti il trattamento che lo riguarda così da metterlo in condizioni di prestare il consenso con la necessaria consapevolezza.

La previsione del consenso informato se pur tesa a rafforzare la tutela degli utenti, non appare del tutto idonea a garantire la protezione dei dati personali dei minori.

Non è di scarso rilievo, infatti, con riferimento ai dati particolari, quelli che riguardano la sfera più intima della persona, i c.d. dati sensibili, che l'art.9 del GDPR nel sancire un generale divieto di trattamento con riferimento di questa particolare categoria di dati, tra le possibili cause di deroga al divieto, individui, il consenso esplicito prestato dall'interessato e l'ipotesi in cui il trattamento "riguardi dati personali resi manifestamente pubblici dall'interessato, quali potrebbero essere quelli postati sui social networks . Si deve presupporre, pertanto, che la presenza di un consenso esplicito o implicito, ricavato dal fatto concludente della pubblicazione, renda legittimo il trattamento.

In considerazione della probabilità di scarsa consapevolezza del minore, invero, sarebbe stato preferibile subordinare la liceità del trattamento al previo consenso esplicito o all'autorizzazione dei genitori esercenti la responsabilità genitoriale.

Il GDPR punta molto sul'adempimento degli obblighi informativi anche con specifico riferimento al trattamento dei dati legato alla circolazione mediante l'attività di profilazione per finalità di marketing. V'è una espressa previsione di un obbligo di informazione esplicita, chiara e separata da qualsiasi altra. Si tratta di un rafforzamento della tutela degli utenti che, tuttavia, non risulta del tutto idonea a garantire in modo efficace soggetti vulnerabili come i minori.

Di fatto, manca una specifica norma che, espressamente, escluda i minori dall'attività di profilazione.

Il secondo comma dell'art. 22 GDPR, infatti, nel prevedere il consenso esplicito tra le cause che legittimano le decisioni automatizzate, incluse le profilazioni - altrimenti vietate dal primo comma dell'articolo stesso – non pone distinzione tra adulti e minori e ciò, sebbene nel Considerando 71 sia indicato, chiaramente, che le decisioni automatizzate e le profilazioni non dovrebbero applicarsi ai minori.

A tal proposito, si deve evidenziare che l'obbligo del titolare del trattamento di attivarsi per verificare con ogni mezzo che il consenso sia validamente prestato, non è garanzia adeguata a scongiurare l'ingresso nei social e nelle piattaforme digitali da parte di minori con età inferiore a quella legale; la verifica infatti, risulta complessa e

in concreto, si riscontra una continua elusione dell'età minima per accedere ai servizi offerti dalle varie piattaforme digitali, social networks, video giochi on line.

E' innegabile che, in concreto, vi sia un'elevata esposizione agli algoritmi di profilazione da parte di un numero sempre crescente di minori con età anche inferiore a quella legale; minori che, profilati alla stessa stregua degli adulti, vengono inconsapevolmente inseriti all'interno di "clusters", ossia classi o gruppi di individui creati dall'algoritmo sulla base di associazioni di aspetti in comune tra i vari soggetti analizzati. Lo sfruttamento dell'immane mole di dati lasciati in rete, infatti, consente agevolmente di tratteggiarne l'identità digitale e di ingabbiarli in percorsi con meccanismi di natura emotiva. Ne è un valido esempio, il caso della class action intentata contro facebook per il video gioco on line che spingeva bambini – profilati e categorizzati come ad alto rischio di spesa - ad acquistare crediti per avanzare nel videogioco senza che vi fosse una chiara e netta distinzione tra il gioco e la reale spesa di danaro.

In questo caso la profilazione delle preferenze dei minori era chiaramente orientata al business e quindi a forzare le preferenze di gioco con meccanismi di natura emotiva che inducevano i bambini all'acquisto.

Il caso del videogioco on line è solo uno dei tanti esempi di come i bambini siano facili cavie per sperimentare la forza degli algoritmi di profilazione e di come gli algoritmi predittivi, possano divenire produttivi del comportamento che avevano predetto, incidendo sulla libertà di autodeterminazione dell'individuo.

E' chiaro che si tratta di un fenomeno di enorme portata che comprende anche la diffusione della disinformazione e della manipolazione politica sui social.

Non è chiaro - anzi è proprio questo uno dei temi del momento - se i codici di condotta, se l'autoregolamentazione sia sufficiente, oppure se lo Stato o organizzazioni internazionali debbano avere un ruolo più incisivo per direzionare meglio un fenomeno che è globale per sua stessa natura e, peraltro, talvolta, anche manovrato da soggetti collegati a Stati non democratici, come nel caso di Tik Tok che di certo, non ha tra le priorità, la tutela dei minori occidentali.

Nei confronti di Tik Tok l'Autorità Garante della Privacy nel marzo 2020, ha avviato un'istruttoria contestando al social la non conformità, di una serie di trattamenti di dati effettuati, al nuovo quadro normativo in materia di protezione dei dati personali.

In particolare il Garante contesta a Tik Tok :

1.il divieto di iscrizione al di sotto dei 13 anni, stabilito dal social network, risulta facilmente aggirabile con l'utilizzo di dati anagrafici falsi (non è previsto come accade per l'iscrizione in altri social un ulteriore step di riconoscimento attraverso un documento di identità). Non viene quindi

verificata l'età minima di 14 anni o il consenso dei genitori e di fatto non è impedita l'iscrizione al social da parte dei più piccoli.
2.L'informativa rilasciata agli utenti è standardizzata; non è prevista una sezione dedicata ai minori che preveda un informativa con un linguaggio più semplice e con meccanismi di alert che segnalino i rischi ai quali si espongono.
3.I tempi di conservazione dei dati risultano indefiniti rispetto agli scopi per i quali vengono raccolti né appaiono indicate le modalità di anonimizzazione che il social network afferma di applicare.
4.In ultimo ma di non minore rilevanza, il social preimposta il profilo dell'utente come "pubblico" pertanto, tutti i contenuti pubblicati sono pubblici, visibili a tutti e potenzialmente anche a chi non è iscritto al social. Tale impostazione predefinita si pone in contrasto con la normativa sulla protezione dei dati che impone l'adozione di misure tecniche ed organizzative che garantiscano, di default, la possibilità di scegliere se rendere o meno accessibili dati personali ad un numero indefinito di persone.

Anche dal caso Tik Tok emerge con chiarezza lo sbilanciamento tra lo strapotere dei soggetti digitali e la posizione degli utenti della rete ed in particolare di quelli più fragili.

Servono, evidentemente, nuove e maggiori tutele e garanzie.

Allo stato, le parole chiave sono Responsabilità ed Educazione Digitale quest'ultima, importantissima per stimolare l'acquisizione delle competenze necessarie ad un utilizzo più consapevole della rete.

Un ruolo fondamentale è giocato dalla famiglia e dalla scuola ma è comunque, necessario che sia sviluppata una responsabilità condivisa da tutti i protagonisti, *in primis,* dalle piattaforme, ma anche dai creatori di contenuti e dagli sponsor.

Avv. Rosa De Caria