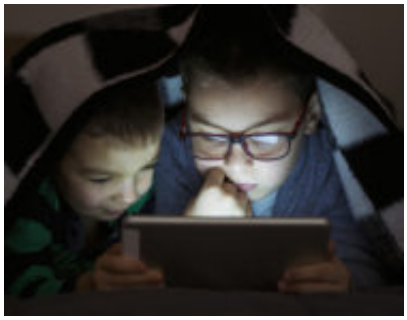
L’età del “consenso digitale” e il delicato rapporto tra minori e sicurezza online

Date : 8 novembre 2017



L’adozione del Regolamento Generale sulla Protezione dei Dati (GDPR) [1] introduce all’art. 8 nuove e specifiche previsioni relative alle “*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*”. In particolare, l’art. 8.1 introduce la regola generale per cui il cd. “**consenso digitale**” applicato alla fornitura di servizi online per ragazzi *under* 18 sarà **lecito solo laddove il minore “*abbia almeno 16 anni*”**. Nel caso in cui, invece, l’interessato abbia un’età inferiore, il trattamento viene considerato lecito “*soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*”.

Tuttavia, lo stesso art. 8.1 prevede una deroga al limite minimo di età per poter considerare valido il consenso al trattamento dei dati rilasciato dal minore, precisando che “***Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni***”.

Nel corso del presente articolo si andranno ad analizzare alcuni degli impatti della mancata adozione di una legge nazionale che fissi a 13 anni l’età per il consenso digitale dal punto di vista dei *provider* di servizi. Si tratta, infatti, di conseguenze che riguardano la possibile esposizione dei minori a contenuti inadeguati e una drastica riduzione delle misure di sicurezza offerte dai provider. Da non sottovalutare, poi, gli aspetti giuridicamente rilevanti in termini di rispetto dei diritti dei minori (intesi anche come tutela della loro sfera personale) e di *compliance* aziendale, che sembrano essere maggiormente favoriti dall’adozione di una legge nazionale e dal suo bilanciamento con eventuali codici di condotta e meccanismi di autoregolamentazione.

Innanzitutto, è bene partire da una considerazione di tipo psico-sociale. La Convenzione sui diritti dell’infanzia e dell’adolescenza, nel trattare argomenti quali la libertà di espressione, associazione, riunione e pensiero del minore, fa riferimento alla sua **capacità di “discernimento”**. Per comprendere quale sia la fase della crescita in cui un under 18 acquisisce siffatta capacità, è utile tenere conto, a titolo esemplificativo, dello studio condotto dal centro pediatrico Stanford Children's Health [2] che ha dimostrato come tra i 12 e i 18 anni l’adolescenza si manifesti con lo sviluppo del cd. pensiero complesso, caratterizzato da operazioni logiche formali che permettono al minore di pensare a diverse possibilità, di ragionare a partire da informazioni conosciute, di considerare diversi punti di vista dibattendo su

idee e opinioni, fino ad arrivare a prendere decisioni autonome e personali. La transizione verso i 13 anni (12, secondo il centro statunitense) riflette tutte queste capacità e necessità.

Appare condivisibile, poi, la perplessità di Janice Richardson, esperta dell'ITU (International Telecommunications Union) e del Consiglio d'Europa e Coordinatore dello European Safer Internet network. Richardson, infatti, d'accordo con alcune organizzazioni per la tutela dei minori in Spagna, Gran Bretagna, Danimarca, Italia, Svezia ecc., ha elaborato un'attenta riflessione [3] sulle conseguenze psico-sociali dell'applicazione dell'art. 8.1. Il tipo di incoraggiamento che gli adolescenti riceverebbero dalla fissazione dell'età minima a 16 anni sarebbe quello a **mentire** sulla propria età in modo da continuare o iniziare a utilizzare comunque la rete e le sue piattaforme, anche nella fascia d'età 13-15. Il discorso di Richardson è molto chiaro: fino ad oggi, i ragazzi dai 13 anni in su sono stati abituati ad accedere ai servizi online, a prescindere dalle norme più o meno restrittive nei vari Paesi. Un irrigidimento della legislazione risulterà con molta probabilità nelle false dichiarazioni da parte degli under 16, che tenderanno ad adottare questo metodo pur di non chiedere il consenso ai genitori. In effetti, nel report redatto alla fine del 2014 da Net Children Go Mobile [4] è emerso che in diversi paesi europei – tra cui l'Italia – **l'utilizzo di internet è diffuso sin dai nove anni e un terzo degli utenti globali di Internet sono di età inferiore ai 18 anni, dove il 68% di loro ha un'età compresa tra i 9 e i 16 anni**.

Date queste premesse, ci si chiede: per rendere il web più sicuro e adatto ai giovani o giovanissimi è utile e necessario fissare a 16 anni l'età per il consenso digitale?

Dal punto di vista dell'**offerta di contenuti idonei da parte dei *provider* di servizi**, la risposta sembra essere negativa. Supponiamo che non venga adottata una legge nazionale per portare a 13 anni l'età del consenso digitale e prendiamo come riferimento i 9 anni quale età di inizio del contatto tra ambiente digitale e bambino (dati di Net Children Go Mobile): un minore ha 10 anni e, come già succede, mente dichiarando di averne 16. La già menzionata ricerca dello Stanford Children's Health spiega che vi è una differenza abissale tra la fase dello sviluppo cognitivo (6-12 anni) e quella dell'adolescenza intermedia (tra i 14 e i 16 anni circa). Infatti, se nella fase medio-adolescenziale si inizia a dare forma a un proprio "codice etico", a valutare le proprie azioni nel lungo termine, quindi a comprenderne le conseguenze e a intessere relazioni più evolute con l'altro, a 10-12 anni il minore è ancora nella fase del cd. pensiero concreto e non ha certo sviluppato una coscienza critica così approfondita come quella di un sedicenne.

Supponiamo, ora, che invece venga adottata una legge nazionale e che, quindi, il bambino di 10 anni di cui sopra menta e dichiari di averne 13 per accedere ai servizi online. Nella fase iniziale dell'adolescenza (12-14 anni), si sviluppa un pensiero fatto di operazioni logiche grazie al quale il minore riesce a prendere decisioni autonome negli ambienti scolastici e familiari, inizia a formare un proprio pensiero e una propria idea su una vasta gamma di argomenti: è sostanzialmente l'immediata evoluzione del pensiero concreto (6-12 anni).

Qual è il punto? Il punto è che rischiare che un minore menta e dichiari di avere 16 anni, avendone magari 10 o anche 13, lo condurrà ad entrare in contatto con contenuti sicuramente inadeguati rispetto alla sua evoluzione cognitiva. Mantenendo la previsione dell'art. 8.1, **i contenuti diventerebbero "standard"** per la sola fascia di età compresa tra i 16 e i 17 anni,

senza più prevedere la loro diversificazione così come avviene oggi (ad es. sui principali social network) in funzione di un'età che varia dai 13 ai 17 anni. Considerati i dati relativi all'uso della rete da parte degli under 13, se un bambino tra i 9 e i 15 anni mentisse, la forbice tra offerta di servizi e contenuti (per over 16) e domanda del minore (under 13) si divaricherebbe notevolmente rispetto a quella odierna (13 anni) che consentiva di proteggere il più possibile anche gli under 13 che mentivano sulla loro età per accedere ai servizi offerti.

Dal punto di vista dei ***service provider*** **con riferimento alla sicurezza dei minori in rete**, la situazione non sembra molto diversa da quella relativa all'idoneità dei contenuti. Infatti, determinare una nuova soglia d'età per la validità del consenso digitale implica che i fornitori di servizi online ne tengano conto. Ciò comporterebbe un riadeguamento sostanziale, poiché formalmente i provider non sarebbero più tenuti a sviluppare strumenti rivolti anche ai più giovani (13-15 anni) utili alla loro sicurezza personale online e potrebbero persino decidere di tagliare fuori quella fetta di utenti, ad esempio, per problemi nell'implementazione di sistemi di verifica del consenso genitoriale. Al contrario, facilitare l'accesso dei minori al web significa incoraggiare le imprese del settore ICT a continuare a mantenere il livello della tutela più alto possibile, non solo per una questione di *compliance* con la legge, ma anche e soprattutto per adempiere alla loro responsabilità sociale così da migliorare la loro reputazione e attrarre un numero maggiore di utenti tramite l'implementazione di ***best practices***. Lo dimostrano alcune recenti esperienze, che hanno visto l'adozione di servizi disegnati appositamente per i bambini in modo da assicurare loro il contatto solo con contenuti positivi e appropriati, in un ambiente sicuro, come è avvenuto con YouTube Kids.

Pensare a un mondo digitale in cui gli under 16 sentano di dover mentire pur di avere accesso alla rete rende molto difficile per i fornitori di servizi offrire contenuti e strumenti idonei. Così verrebbe meno la possibilità di aiutarli a vivere un'esperienza online sicura e *privacy-friendly*, senza dover assumere un'altra identità – quantomeno anagrafica.

Un ultimo e interessante aspetto riguarda il **rapporto tra tutela dei minori online e regolazione relativa ai fornitori di servizi della società dell'informazione e la *compliance* degli stessi**.

L'istituzione, da parte dell'Unione Europea, del programma "Better Internet for Kids" [5] ha l'obiettivo di promuovere un ambiente online più sicuro attraverso l'attuazione di iniziative di autoregolamentazione tra le parti interessate. E in effetti, assieme alla questione dei contenuti e delle *best practices*, di cui si è parlato in precedenza, risulterebbe ben più funzionale alla salvaguardia dei più giovani che navigano sul web spostare l'attenzione dall'"aumento età del consenso del minore" all'adozione virtuosa di pratiche condivise da parte dei fornitori di servizi della società dell'informazione. Come fare? Il GDPR può offrire una soluzione tramite i **codici di condotta**, introdotti con il GDPR ex art. 40. È proprio quest'ultimo, alla lettera g) del secondo paragrafo, a specificare che "*Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a* […] *g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore*". Il privilegio dei codici di condotta è quello di fare un passo verso l'*enforcement* delle buone pratiche che

non hanno di per sé natura obbligatoria. Infatti, il Considerando 77 del RGPD precisa che "*l'individuazione di migliori prassi per attenuare il rischio* [potrebbe] *essere* [fornita] *in particolare mediante codici di condotta approvati*". Ciò significa che, introducendo le "buone pratiche" in un codice di condotta approvato dalle autorità di controllo, gli impegni sulla sicurezza dei minori online diventerebbero vincolanti per i titolari e i responsabili del trattamento al fine di ottemperare alle disposizioni del codice stesso e, quindi, del GDPR.

Mantenendo aperta la questione dei "codici di condotta", è necessario tornare per un istante all'art. 8.1 del GDPR: "*Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni*". Ciò significa che ogni Stato membro avrà la sua legge e chi non legifererà si allineerà automaticamente alla soglia minima dei 16 anni per la validità del consenso digitale. Diverse le regole, quindi, in ciascuna nazione europea e diverse anche rispetto a quelle applicate negli Stati Uniti, dove non solo sono stabiliti territorialmente moltissimi fornitori di servizi web, ma con il Children's Online Privacy Protection Act (COPPA) [6], l'età del consenso in rete è già fissata a 13 anni.

A questo punto, gli scenari che si aprono in Europa sono due: da un lato, i service provider esteri potrebbero decidere di tagliare fuori la fetta di utenti (13-15 anni) per i quali sarebbe richiesta l'implementazione di farraginosi sistemi di verifica del consenso genitoriale. In casi estremi, potrebbero perfino cessare la prestazione del servizio nei paesi UE che non abbiano adottato la legge nazionale che fissi a 13 anni l'età per il consenso digitale. Così, si penalizzerebbe non solo il diritto di accesso degli adolescenti tra i 13 e i 15 anni, ma anche la stessa **offerta di libero mercato dei servizi online**. In secondo luogo, all'interno della stessa UE, il medesimo trattamento di dati di minori potrebbe risultare lecito o illecito a seconda della legge nazionale applicabile e si presenterebbe la necessità di effettuare una continua mediazione tra la soglia fissata dalla legge nazionale del minore e quella fissata dalla legge dello Stato di stabilimento del titolare. Per ovviare al problema dell'età del consenso diversa e diversificata in Europa, rientra quindi in gioco il codice di condotta come strumento di tutela concreta. Questo, infatti, non solo risolverebbe la questione **dell'*enforcement* delle buone pratiche**, ma offrirebbe anche una soluzione in termini di **estensione territoriale del codice** stesso. All'art. 40.7 del GDPR, infatti, viene introdotta la possibilità per le "*associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento*" di adottare un codice per attività di trattamento che avvengano in diversi Stati membri. Inoltre, con atto di esecuzione della Commissione Europea, il codice potrebbe acquisire validità generale in tutta l'Europa ex art. 40.9 GDPR.

Considerati dunque i profili psico-sociali della questione, assieme a quelli relativi alla sicurezza e a quelli giuridicamente rilevanti, l'adozione di una legge nazionale che fissi l'età per il consenso digitale a 13 anni sembra essere la migliore garanzia a tutela dei minori per ciascuno degli aspetti menzionati (sociali, giuridici, di sicurezza) anche in termini di apertura del libero mercato dei servizi online.

Bibliografia:

1. Regolamento (UE) 2016/679, in http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

2. http://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594
3. http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16
4. http://netchildrengomobile.eu/reports/
5. https://ec.europa.eu/digital-single-market/safer-internet-better-internet-kids
6. https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy

Per approfondimenti, L. Bolognini, C. Bistolfi, L'ETA' DEL CONSENSO DIGITALE - Privacy e minori on line, riflessioni sugli impatti dell'art. 8 del Regolamento 2016/679(UE), in http://anticyberbullismo.it/wp-content/uploads/2017/06/Et%C3%A0_del_consenso_digitale_IIP_CNAC_2017.pdf

A cura di: **Camilla Bistolfi**