L'ETA' DEL CONSENSO DIGITALE

Privacy e minori on line, riflessioni sugli impatti dell'art. 8 del Regolamento 2016/679(UE)

di Luca Bolognini (l.bolognini@istitutoprivacy.it)
e Camilla Bistolfi (c.bistolfi@istitutoprivacy.it)

Roma, 7 marzo 2017

Uno studio dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati
www.istitutoitalianoprivacy.it
e del Centro Nazionale Anti-Cyberbullismo (CNAC)
www.anticyberbullismo.it

Sommario

Sintesi

L'adozione del Regolamento Generale sulla Protezione dei Dati (RGPD) introduce all'art. 8 nuove e specifiche previsioni relative alle "*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*".
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 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 lavoro vengono prese in esame le diverse ragioni che evidenziano come **un più elevato limite minimo di età per la validità del consenso digitale del minore non pare essere la migliore forma di tutela** e, per questo, viene proposto un approccio più realistico dal punto di vista sociale e giuridico, in modo da garantire effettivamente la tutela dei diritti dei minori e la loro sicurezza.
In tal senso, sono stati individuati una serie di elementi che dimostrano l'auspicabilità dell'adozione di una **legge nazionale che fissi a 13 anni l'età per il consenso digitale** autonomamente fornito dal minore, tra cui:

- I diritti internazionalmente riconosciuti ai minori e le loro capacità cognitive nella fascia di età compresa tra i 13 e i 17 anni, ma anche in quella tra i 9 e i 12;
- Le possibili conseguenze fattuali della mancata adozione di una legge nazionale che fissi a 13 anni l'età per il consenso digitale, conseguenze che riguardano non solo il piano educativo e della consapevolezza dei minori, ma anche e soprattutto la loro possibile esposizione a contenuti inadeguati e una drastica riduzione delle misure di sicurezza offerte dai provider;
- 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.

Considerati dunque i profili sociali della questione, assieme a quelli relativi alla sicurezza e a quelli giuridicamente rilevanti, si propone di seguito l'analisi approfondita di ciascuna delle circostanze che rendono, a parere degli autori, l'adozione di una legge nazionale (nel caso italiano, mediante previsione di un articolo *ad hoc* nella legge di delegazione europea 2017 o 2018) - che fissi l'età per il consenso digitale a 13 anni - la migliore garanzia a tutela dei minori per ciascuno degli aspetti menzionati (sociali, giuridici, di sicurezza).

1) Introduzione all'articolo 8 del Regolamento Generale sulla Protezione dei Dati: l'età per il consenso digitale dei minori.

La prima delle condizioni di liceità del trattamento, fissata dall'art. 6.1.a) del Regolamento Generale sulla Protezione dei Dati UE (Reg. 2016/679(UE), di seguito "RGPD"), è costituita dal consenso dell'interessato, con il quale egli "*manifesta l'**intenzione libera, specifica, informata e inequivocabile** di accettare il trattamento dei dati personali che lo riguardano*" (Considerando 32, RGPD).

Riprendendo le disposizioni dell'art. 6.1.a), l'art. 8 RGPD introduce una specifica previsione relativa alle "*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*". Si tratta, sostanzialmente, di quel consenso conosciuto come "consenso digitale", legato alla fornitura di servizi online a ragazzi che non hanno ancora compiuto la maggiore età.

In particolare, l'art. 8.1 specifica che, nel caso in cui vengano offerti a minori i predetti servizi, il loro consenso 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*". Ciò implica che un minore non ancora sedicenne, senza l'obbligatorio consenso di un genitore o del tutore, non potrà iscriversi a qualsiasi sito web – inclusi i social media come social network o piattaforme di condivisione dei contenuti – che raccolga i suoi dati personali.

L'intenzione del legislatore europeo è indubbiamente quella di proteggere bambini e ragazzi giovanissimi dalla raccolta e dal trattamento dei loro dati personali, "*in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali*", come ricorda il Considerando 38. Quest'ultimo presta anche una particolare attenzione alla sovraesposizione a messaggi commerciali/pubblicitari e alla profilazione effettuata sui minori proprio perché le decisioni basate "*unicamente sul trattamento automatizzato, compresa la profilazione*", *ex* art. 22, possono produrre effetti giuridici o incidere in modo significativo sull'interessato, avendo ripercussioni anche postume, nell'età adulta. Sovviene, in proposito, la metafora del celebre psicoanalista ungherese Sándor Ferenczi, per cui "*dove sia accesa soltanto una candela basta una mano davanti alla sorgente di luce per oscurare metà della stanza; la stessa cosa accade col bambino: se gli arrecate un danno se pur minimo agli inizi potrà proiettare un'ombra su tutto il resto della sua vita*"[1]. In questo senso, il Considerando 65, riguardante il diritto alla cancellazione dei propri dati, accentua la rilevanza dell'oblio qualora l'interessato abbia prestato il proprio consenso "*quando era minore, e quindi **non pienamente consapevole dei rischi** derivanti dal trattamento*" *ex* art. 8.1 (cfr. art. 17.1.f).

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

[1] Ferenczi S. (1927), L'adattamento della famiglia all'individuo. In Carloni G. e Molinari (a cura di) Opere di S. Ferenczi. Guaraldi Ed.

Dunque, in via generale l'età per il consenso digitale "autonomo" è stabilita a 16 anni, ma essa è riducibile qualora il Paese europeo decida di adottare una legge nazionale per portarla sino a 13 anni.

Definiti sommariamente tutti gli elementi dell'art. 8, e pur tenendo a mente il fine ultimo della loro adozione, nel presente lavoro vengono riportate alcune riflessioni che conducono a considerare auspicabile l'adozione di una legge nazionale che fissi a 13 anni l'età per il consenso digitale autonomamente fornito dal minore, *ex* art. 8.1 RGPD. Come si vedrà di seguito, malgrado superficiali apparenze, **un più elevato limite minimo di età per la validità del consenso digitale del minore non pare essere la migliore forma di tutela**. Si noti che l'obiettivo di questo elaborato non è certo quello di promuovere l'abolizione di una soglia definita, il cui valore è invece riconosciuto già da molti anni da molti *stakeholder* della società dell'informazione. Piuttosto, di seguito verranno prese in esame le diverse ragioni che evidenziano la bontà di un approccio realistico e praticabile, dal punto di vista sociale e giuridico, della tutela dei diritti dei minori e da quello relativo alla loro sicurezza.

Sintesi della normativa

Art. 8.1 RGPD sulle "*Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*":

- **Regola generale** per il consenso digitale: "***il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni***. *Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*".

- Deroga alla regola generale: "***Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni***".

2) 13 o 16 anni? Uno sguardo ai diritti e alle capacità cognitive degli *under* 18

Il RGPD, considera lecito, nell'ambiente online, il trattamento dei dati personali basato sul consenso di un minore solo qualora egli abbia almeno 16 anni: nell'età compresa tra i 13 e i 15 anni, spetterà al genitore fornire il predetto consenso.

Cosa s'intende per "trattamento di dati personali di un minore"? A ben vedere, seguendo il disposto dell'art. 8.1 combinato con la definizione di trattamento di cui al precedente art. 4(2), il trattamento di dati personali, per cui è richiesto il consenso del genitore per un ragazzo sotto i 16 anni, dovrebbe consistere nella raccolta ed elaborazione delle informazioni riferibili a un minore identificato o identificabile, anche indirettamente, per tutto ciò che viene offerto sulla rete in termini di servizi: dall'attivazione di un indirizzo e-mail, all'acquisto di regali per genitori o amici a, ancora, iscriversi a siti che consentono di effettuare ricerche (ad es. scolastiche) o a un social network o a una piattaforma di condivisione di contenuti.

Giova ricordare, in proposito, che l'art. 13.1 della Convenzione sui diritti dell'infanzia e dell'adolescenza[2] (di seguito, "CDIA") sancisce che: "*Il fanciullo ha diritto alla libertà di espressione. Questo diritto comprende la* ***libertà di ricercare, di ricevere e di divulgare informazioni e idee*** *di ogni specie, indipendentemente dalle frontiere, sotto forma orale, scritta, stampata o artistica,* ***o con ogni altro mezzo a scelta del fanciullo***". La rete non è forse un "*altro mezzo*"? L'unico strumento che può limitare l'esercizio di questo diritto è una legge adottata ai soli fini di "*rispetto dei diritti o della reputazione altrui*" oppure della "*salvaguardia della sicurezza nazionale, dell'ordine pubblico, della salute o della moralità pubbliche*", come indicato dallo stesso art. 13, al secondo comma.
Sulla stessa linea si muove anche l'art. 15, relativo al diritto "*alla* ***libertà di associazione*** *e alla* ***libertà di riunirsi pacificamente***". Usare i social network o le piattaforme e aderire alle community è, indubbiamente, un modo per esercitare la libertà di associarsi e riunirsi pacificamente.
Anche nel caso dell'art. 15, solo una legge può stabilire delle limitazioni a questi diritti, "*necessarie in una società democratica nell'interesse della sicurezza nazionale, della sicurezza o dell'ordine pubblico, oppure per tutelare la sanità o la moralità pubbliche, o i diritti e le libertà altrui*" (art. 15.2).

Ancora, la formula usata dall'art. 12.1 della CDIA e quella dell'art. 14 aggiungono importanti elementi su cui riflettere. L'art. 12.1 garantisce al "*fanciullo* ***capace di discernimento*** *il diritto di esprimere liberamente la sua opinione su ogni questione che lo interessa*". In parallelo, l'art. 14, sancisce il diritto "*alla libertà di pensiero, di coscienza e di religione*" fermo restando "*il diritto e il dovere dei genitori oppure, se del caso, dei tutori legali, di guidare il fanciullo nell'esercizio del summenzionato diritto* ***in maniera che corrisponda allo sviluppo delle sue capacità***". Dunque, combinando le due disposizioni, un minore sviluppa progressivamente le "*sue capacità*", diventando "*capace di discernimento*", ma, ancora una volta, quand'è che egli acquisisce la capacità di esercitare autonomamente i diritti di cui agli artt. 13 e 14 della CDIA? Ciò avviene già a 13 anni o è necessario attendere sino ai 16? Si potrebbe pensare che dipenda dal minore, dalla sua educazione, dalla sua velocità di sviluppo.

A tal proposito, si giunge ad un ulteriore spunto di riflessione, ossia quello favorito da una ricerca – tra le tante prodotte sino ad oggi in materia e senza pretesa di esaustività, ma solo di esemplificazione – sullo sviluppo cognitivo dei minori, condotta dall'importante centro pediatrico Stanford Children's Health[3] che evidenzia come vi siano determinate fasi tipiche nella crescita di un bambino/adolescente. Tra i 6 e i 12 anni, troviamo la fase del cd. sviluppo cognitivo concreto, relativo alla capacità di pensare e ragionare, effettuando operazioni concrete su oggetti e azioni (ad es. addizionare, sottrarre, ordinare ecc.). Tra i 12 e i 18 anni, invece, si esprime l'adolescenza con lo sviluppo del cd. **pensiero complesso**, caratterizzato da operazioni logiche

[2] http://www.unicef.it/doc/599/convenzione-diritti-infanzia-adolescenza.htm.
[3] http://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594.

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. Per questa ragione, i pediatri e gli esperti di Stanford incoraggiano gli adolescenti a condividere i propri pensieri e gli adulti a includerli nelle discussioni che riguardano una vasta gamma di argomenti, problemi ed avvenimenti, e a far sì che sviluppino in modo indipendente le loro idee[4]: la rete è di fatto un luogo in cui **sviluppare le capacità personali e relazionali**, comunicando e gestendo rapporti, ma anche esercitando il diritto di espressione e di informazione.
In sostanza, attenendosi all'approccio puramente "medico-scientifico", già a 13 anni il minore è nel pieno dello sviluppo della sua identità personale e, per questo, è di norma "*capace di discernimento*" anche per quanto riguarda l'uso dei servizi della società dell'informazione.

In sintesi:

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 che ha dimostrato come:

- Tra i 6 e i 12 anni, avviene il cd. sviluppo cognitivo concreto, relativo alla capacità di pensare e ragionare, effettuando operazioni concrete su oggetti e azioni (ad es. addizionare, sottrarre, ordinare ecc.);

- Tra i 12 e i 18 anni, invece, l'adolescenza si manifesta 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.

In sostanza, attenendosi all'approccio puramente "medico-scientifico", **già a 13 anni il minore è nel pieno dello sviluppo della sua identità personale e, per questo, è di norma "*capace di discernimento*" anche per quanto riguarda l'uso dei servizi della società dell'informazione**.

[4] Ibid.

3) In attesa di una legge nazionale: le possibili conseguenze di una "anziana" età minima per il consenso digitale

Posto che sul piano cognitivo è la dottrina scientifica stessa a fornire basi per la collocazione dell'asticella per la validità del consenso digitale al di sotto dei 16 anni, va comunque affrontata la questione della sicurezza di Internet per i minori. Per quanto un adolescente sia "*capace di discernimento*", e pur essendo le nuove generazioni estremamente abili nell'uso della rete, è assolutamente condivisibile la preoccupazione del legislatore europeo quando cerca di **rendere il web più sicuro e adatto ai giovani o giovanissimi**. Ma è utile e necessario, per tali nobili obiettivi, fissare a 16 anni l'età per il consenso digitale?

Per rispondere a questa domanda, sono state prese in esame diverse conseguenze che un'età minima troppo elevata comporterebbe. Si tratta di effetti collaterali di una scelta apparentemente logica, che impattano sull'educazione, sulle dinamiche sociali dei minori e persino sulla stessa sicurezza della rete e che verranno illustrati in estrema sintesi di seguito.

3.1 La questione dell'educazione e della consapevolezza digitale

È piuttosto evidente che, pur aumentando l'età minima di validità del consenso, non si impedisce *de facto* l'accesso ai contenuti "dannosi" di circolare in rete, e tantomeno si tutelano gli adolescenti *over* 16 dalla ricezione degli stessi. I temi centrali della discussione dovrebbero essere due: quello relativo ai **contenuti offerti dalla società dell'informazione** (per il quale si rimanda ai paragrafi 3.2 e 3.3) e, soprattutto, quello dell'**educazione dei minori al corretto uso della rete**. Considerare la questione "risolta" e la sicurezza "ripristinata" dopo aver impedito l'accesso autonomo ai servizi digitali alla fascia di età 13-15 significa ragionare in astratto, negando un fenomeno anziché affrontandolo nel merito, senza tenere conto delle implicazioni concrete di una scelta così restrittiva.

Le ragioni di questa considerazione sono varie e rispondono a criteri di realismo: *in primis*, nel report redatto alla fine del 2014 da Net Children Go Mobile[5] è emerso che in diversi paesi europei – tra cui ovviamente l'Italia – **l'utilizzo di internet è diffuso sin dai nove anni** e già dagli 8 molti ragazzi posseggono uno *smartphone* regalato dai genitori. Sul tema, in occasione del XIII Safer Internet Day 2017, la Giornata per la sicurezza in Rete istituita e promossa dalla Commissione Europea, Telefono Azzurro ha organizzato, alla Camera dei Deputati, l'evento "Il rapporto tra i giovani e internet"[6] – cui hanno partecipato diversi rappresentanti delle istituzioni, di aziende e di importanti realtà del mondo della rete. In questa sede è stata presentata in anteprima un'indagine realizzata da Doxa Kids per Telefono Azzurro, dalla quale è emerso che, in Italia, tra gli *under* 13 intervistati (su un campione di oltre 600 adolescenti) il 73 % usa abitualmente Whatsapp, il 44% Facebook, seguito da Instagram al 35%, Snapchat al 13% e Twitter all'11%.

In realtà, questi dati non devono sorprendere: è normale che in una società digitale i giovanissimi siano attratti dalla tecnologia e dalla rete, tanto più che prima ancora di possedere un cellulare

[5] http://netchildrengomobile.eu/reports/.
[6] http://www.azzurro.it/it/content/safer-internet-day-06022017-1.

entrano in contatto con il computer domestico o con le consolle di videogiochi che ormai richiedono necessariamente una connessione a internet. Questi dati, peraltro, mostrano con chiarezza come i nativi digitali, molto più degli adulti, siano in grado di **aggirare le limitazioni della rete** per creare profili o account anche nella fascia di età che va dai 9 ai 12 anni.
Alla luce di queste considerazioni, il dato che dovrebbe destare sconcerto non è quello sull'uso dei servizi della società dell'informazione sin dalla tenera età. Piuttosto, fatte salve alcune iniziative[7], il problema sembra essere la pressoché totale **inesistenza di un programma di formazione incluso nella didattica** che educhi i minori a un utilizzo sicuro delle tecnologie digitali. La ricerca dell'European Schoolnet nell'ambito dell'azione di ricerca SMILE (Social Media in Learning and Education)[8], condotta da oltre cento insegnanti provenienti da tutta Europa, ha evidenziato come la scuola giochi un ruolo importantissimo nella guida di bambini e adolescenti verso un uso sicuro e responsabile delle piattaforme della società dell'informazione. Impedire astrattamente ai ragazzi tra i 13 e i 15 anni di accedere ai servizi della società dell'informazione, come i social network, le piattaforme di condivisione dei contenuti, le e-mail ecc., non farebbe altro che generare un maggiore senso di curiosità nei giovani – che certamente non si fermerebbero dinanzi a una regola facilmente aggirabile – e incentivare un approccio timoroso e ansioso tra gli adulti. Questi ultimi, tra l'altro, potrebbero non possedere le conoscenze culturali, informatiche e linguistiche per comprendere le circostanze del trattamento dei dati dei propri figli o potrebbero essere spaventati all'idea che essi vengano esposti a determinati tipi di contenuti.
Di qui tre riflessioni aggiuntive. La prima è che, per eliminare le ritrosie (a volte lecite) degli adulti, occorre concentrarsi, appunto, sui contenuti e non necessariamente sugli utenti, come si vedrà nel paragrafo 3.2. La seconda riguarda i dati che emergono[9] e di cui si è già parlato, cioè che l'uso della rete è diffuso tanto tra soggetti *over* 16 quanto tra quelli che hanno tra i 9 e i 15 anni e spesso sono proprio i genitori ad autorizzarlo o a favorirlo in generale e *a priori*.
Del resto, la stessa Unione Europea ha rilasciato recentemente alcuni documenti e dati, ottenuti con il supporto di Net Children Go Mobile[10] e del Centre for International Governance Innovation[11], in cui ha evidenziato che **un terzo degli utenti globali di Internet sono di età inferiore ai 18 anni e il 68% di loro ha un'età compresa tra i 9 e i 16 anni** e possiede almeno un profilo su un social network.

---

[7] "*Una vita da social*", iniziativa promossa dalla Polizia di Stato e dal Ministero dell'Istruzione per promuovere la sicurezza nell'uso della Rete tra gli utilizzatori dei social network (in particolare studenti del le scuole secondarie di primo e secondo grado, insegnanti e familiari) in https://www.facebook.com/unavitadasocial/; "*Generazioni Connesse*", progetto coordinato dal Ministero dell'Istruzione e co-finanziato dalla Commissione Europea. Generazioni Connesse agisce come Safer Internet Center Italiano e promuove un utilizzo consapevole delle tecnologie digitali per i più giovani, avvalendosi di un *advisory board* formato dai più noti *stakeholder* pubblici e privati del settore ICT e sicurezza della rete: AGCOM, Garante per la protezione dei dati personali, Facebook, Google, Sky, Poste Italiane, Fastweb, Mediaset, Tim, Vodafone, Wind ecc., in http://www.generazioniconnesse.it/site/it/home-page/.
[8] http://www.eun.org/teaching/smile.
[9] Net Children Go Mobile, Network report, Novembre 2014, in http://netchildrengomobile.eu/reports/.
[10] http://netchildrengomobile.eu/.
[11] https://www.cigionline.org/publications/one-three-internet-governance-and-childrens-rights.

A ben vedere, tenere alta l'età del consenso digitale autonomo non aiuterebbe a prevenire i rischi: tra i 13 e i 15 anni i giovani sentono l'esigenza di ragionare, dibattere e decidere – in virtù di quello che nel paragrafo 2 si è definito come "pensiero complesso" – e, per questo, tenderanno non solo a volere connettersi ma anche ad aggirare i meccanismi e le *policy* che escludono i minori di 16 anni dai servizi *online*, come si vedrà più esaustivamente nel paragrafo 3.2.
Inoltre, la soglia minima per la validità del consenso fornito da un minore non può avere in ogni caso alcun valore se non è accompagnata da un'idonea formazione di coloro cui si decide, *ex* art. 8.1 RGPD, di attribuire la facoltà di prestare il consenso digitale. È auspicabile **formare i minori a prescindere dalla loro età**, per evitare che i più piccoli, eludendo le regole europee o nazionali sul consenso digitale, si ritrovino a fare i conti con i pericoli della rete, senza conoscerli.
A questo punto, è d'obbligo porsi una domanda. Posto che si definiscano i 16 anni come età per considerare valido il consenso digitale autonomo e posto che i minori vengano formati all'uso della rete ben prima del compimento del sedicesimo anno, è realistico pensare che queste misure costituiscano una forma di protezione per i più piccoli (*under* 16)?
La scuola guida per il conseguimento della patente si compone di due fasi. La prima è l'apprendimento teorico delle regole del codice della strada; la seconda è la pratica. Tanto più si guida, maggiore sarà la capacità di applicare e riconoscere le regole del codice. Ebbene, per il web può valere lo stesso ragionamento. Un recente studio condotto da EU Kids Online[12], che si occupa di coordinare e stimolare le indagini relative alle modalità con cui i minori usano i nuovi media, con particolare riferimento ai rischi e alle misure di sicurezza del web, ha tratto la seguente conclusione: **più i ragazzi usano Internet, più acquisiscono competenze digitali** e sono in grado di cogliere le opportunità della rete. D'altra parte, l'esposizione ai contenuti della rete, aiuta a sviluppare anche competenze relative alla sicurezza che, come dimostra il già citato rapporto di Net Children Go Mobile, consistono nella capacità di comparare contenuti e siti web, valutando l'affidabilità delle informazioni.
Più lezioni di guida si prendono con l'istruttore, più si impara a guidare. Più si naviga nel web avendo alle spalle la giusta formazione, più si impara a farlo in maniera sicura e consapevole.
In effetti, la citata ricerca dell'European Schoolnet[13] ha evidenziato il fatto che gli adolescenti (si parla dunque della fascia di età compresa tra i 12 e i 17 anni[14]) sono molto più consapevoli degli adulti rispetto a quali informazioni dovrebbero essere condivise *online*. Essi, infatti, si rendono conto che i diritti digitali sono legati a una serie di responsabilità reali, come la valutazione delle possibili conseguenze delle loro azioni, la responsabilità e l'autocontrollo. Oltretutto, i più recenti fatti di cronaca in materia di cyberbullismo, *sexting*, istigazione all'odio e alla violenza sulle donne, hanno ampiamente dimostrato che l'irresponsabilità nell'uso della rete non è ascrivibile solo a fasce di età inferiori ai 18 anni, anzi.

[12] http://eprints.lse.ac.uk/60512/1/EU%20Kids%20onlinie%20III%20.pdf.
[13] MILE (Social Media in Learning and Education), in http://www.eun.org/teaching/smile.
[14] Cfr. ricerca del Stanford Children's Health, in http://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594.

Un'altra ricerca, condotta dal Pew Research Center, intitolata "*Teens, Social Media, and Privacy*"[15], ha mostrato come il 74% degli oltre 800 adolescenti intervistati abbiano capacità di gestire la propria reputazione *online*, cancellando, se necessario, le persone dalle proprie liste di amici o di *follower*. Tra coloro che usano Facebook, il 60% ha un profilo privato, il 25% un profilo parzialmente privato e la maggioranza conosce e ha capacità di gestire le proprie impostazioni sulla privacy nel social network.

L'educazione all'uso delle piattaforme digitali non è, comunque, l'unico aspetto da considerare in tema di apprendimento: esiste anche l'**educazione tramite le piattaforme digitali**. Si pensi a cosa accadrebbe se tutti i ragazzi al di sotto dei 16 anni dovessero chiedere il permesso ai genitori per utilizzare con un proprio *account* i servizi *online*. Non solo ne risentirebbero molte attività scolastiche, le ricerche, lo sviluppo di capacità critiche e di selezione delle informazioni, ma soprattutto si indebolirebbe lo stesso processo formativo che avviene – esso stesso – tramite l'uso di servizi web. Come si può insegnare agli *under* 16 a utilizzare in modo sicuro il web senza farli accedere ai servizi del web? Gli studenti europei sprovvisti di una legge nazionale che porti a 13 anni l'età del consenso digitale sarebbero fortemente svantaggiati, sul piano educativo e culturale, rispetto ai loro coetanei americani o australiani e si creerebbe un **"*digital divide* europeo"** in termini di accesso alle risorse della rete. Ammesso che il divieto teorico possa reggere alla prova dei fatti, beninteso.

3.2 Attenzione alle bugie e soprattutto ai contenuti!

In una lettera redatta nel dicembre 2015 da esperti del settore ICT e diretta ai membri del Parlamento Europeo[16], **in molti avevano espresso, sin dalla prima modifica dell'art. 8.1 RGPD, le loro preoccupazioni con riferimento all'eccessivo innalzamento dell'età per la validità del consenso digitale – tra essi anche il Telefono Azzurro**, da sempre in prima linea per la difesa dei diritti dei minori e per la loro tutela anche sul web. Oltre a citare alcune delle summenzionate ricerche, come quella condotta dal Pew Research Center, nella lettera si legge la preoccupazione di Janice Richardson, esperto 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 in materia. Il tipo di incoraggiamento che gli adolescenti riceverebbero dalla fissazione dell'età minima a 16 anni sarebbe, semplicemente, 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. I vari

[15] http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/.
[16] http://www.antibullyingpro.com/blog/2015/12/11/letter-expressing-concern-to-the-draft-general-data-protection-regulation-13to16.

firmatari della lettera, a tal proposito, evidenziano come la **burocratizzazione dell'ottenimento del consenso (genitoriale)** finirebbe per precludere, a quei ragazzi che non intendono aggirare le regole, l'accesso a tutta una serie di risorse e informazioni che, ormai, sono reperibili quasi esclusivamente in rete. Inoltre, riprendendo quanto già affermato nei paragrafi 2 e 3.1, non servono particolari conoscenze sulla natura umana per capire che proibire ai ragazzi tra i 13 e i 15 anni, nel pieno dell'adolescenza, di accedere ai servizi della società dell'informazione come i social network, le piattaforme di condivisione dei contenuti, le e-mail ecc., non farebbe altro che destare in loro maggiore curiosità e senso di sfida rispetto al divieto: "**Niente desideriamo di più di quello che non ci è consentito**", citando il drammaturgo Publilio Siro.

Considerato che, anche quando l'età del consenso sia stata fissata a 13 anni, come già accaduto in diverse esperienze nazionali nel mondo, i numeri indicano una enorme presenza di *under* 13 *online* (cfr. paragrafo 3.2), non è difficile immaginare che ciò accadrebbe con perfino maggiore intensità se si precludesse anche alla fascia 13-15 di accedere ai servizi web.
È vero: dichiarandosi più grande e mentendo sull'età, il minore – a prescindere dal fatto che l'età per il consenso sia 13 o 16 anni – rischia di entrare in contatto con contenuti non adatti (ad es. nelle piattaforme di *videosharing*, in cui l'accesso ad alcuni filmati può essere vietato ai minori di 14 anni), quindi tanto vale alzare l'asticella e proteggere gli *under* 16. Ma se i bambini tra i 9 e i 12 anni già mentono, dichiarando di averne 13 e, sicuramente, altrettanto farebbero tra i 13 e i 15, dichiarando di averne 16 (per le ragioni di cui sopra), ha veramente senso innalzare l'asticella?

Per rispondere, bisogna lasciar entrare nel campo della nostra riflessione un altro elemento: i **contenuti**.
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[17]): un minore ha 10 anni, mente e dichiara di averne 16.
Come illustra la già menzionata ricerca dello Stanford Children's Health[18], 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

[17] http://netchildrengomobile.eu/reports/.
[18] http://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594.

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. Diverso è, invece, il gap presente tra i contenuti offerti – dichiaratamente, esplicitamente pensati per quel *target* – a un ragazzo di 13 anni e uno di età compresa tra i 9 (sempre prendendo come riferimento i dati di Net Children Go Mobile[19]) e i 12. I 12-13 anni rappresentano una età di connessione tra l'essere bambini e il diventare adolescenti[20], il che porta a una sostanziale similitudine nei contenuti offerti, non totale, certo, ma comunque ampia.

Ecco, dunque, entrare in gioco la questione dei contenuti, già accennata in precedenza.
Fissare l'età del consenso digitale a 16 anni è più pericoloso di quanto si possa pensare, poiché tutti **i contenuti proposti diventerebbero "standard" per la sola fascia di età compresa tra i 16 e i 17 anni**, senza più prevedere contenuti e servizi diversificati come quelli ad oggi offerti in funzione di un'età che varia dai 13 ai 17 anni. Ad esempio, le principali piattaforme di social network prevedono ad oggi un trattamento specifico in termini di contenuti (inclusa la pubblicità proposta), ma anche di servizi forniti ai minori tra i 13 e i 18 anni, tra cui: by default la geolocalizzazione disabilitata, la condivisione solo con gli amici e il controllo dei tag; l'impossibilità di risalire alle informazioni di contatto del minore tramite motore di ricerca del social; l'alert "in-product" quando il minore sceglie di cambiare la modalità di condivisione da "amici" a "tutti" o quando aggiunge tra gli amici un adulto.
Pertanto, se il bambino di cui sopra (10 anni) mentisse, la forbice tra offerta di servizi e contenuti (per *over* 16) e domanda del minore (*under* 13) si divaricherebbe notevolmente, con tutti i rischi che ne conseguono. Ad esempio, gli verrebbero proposti contenuti anche pubblicitari calibrati su un'età che va dai 16 ai 17 anni, ben distante non solo da quella reale (10 anni), ma anche da quella che, ad oggi, costituiva il limite minimo per iscriversi ai social network (13 anni) e che consentiva di proteggere il più possibile anche gli *under* 13 che mentivano sulla loro età per accedere ai servizi offerti. Come si è sottolineato in precedenza, infatti, la differenza cognitiva tra i 9 e i 13 anni è sicuramente presente, ma è anche certamente molto attenuata rispetto a quella che si crea tra la fascia 9-13 e 16-17.
Sarebbe più semplice gestire la **calibrazione dei servizi offerti** qualora si continuasse a mettere in condizione il minore tra i 13 e i 15 anni di dichiarare la sua età, in modo da **adeguare i contenuti** a questa fascia e restringere parallelamente la forbice tra l'offerta di contenuti *online* e la possibile falsa dichiarazione per ottenere un servizio tra i 9 e i 12 anni.

La questione dell'adeguamento dei contenuti è il cardine dell'intero ragionamento. La restrizione dell'accesso a Internet dovrebbe essere sostituita da un focus sui contenuti che dovranno essere non solo appropriati a seconda delle diverse età, ma anche utili a migliorare le competenze

[19] http://netchildrengomobile.eu/reports/.
[20] http://www.stanfordchildrens.org/en/topic/default?id=cognitive-development-90-P01594.

digitali dei minori e ad agevolarli nello svolgimento sicuro delle loro attività sul web, come si vedrà nel paragrafo 3.3. Due elementi, dunque:

- un'**educazione digitale** che renda i minori in grado di conoscere e riconoscere le trappole della rete, anche e soprattutto quando essi stessi siano generatori di contenuti;
- una **protezione concreta basata sulla fruibilità di contenuti e servizi idonei** per ragazzi di un'età che va dai 13 ai 17 anni per:
    - a) non indurli a mentire sulla loro età pur di accedere ai servizi web;
    - b) non costringerli a rinunciare all'uso della rete sotto i 16 anni per evitare di chiedere il consenso dei genitori;
    - c) fare in modo che, grazie all'adeguamento dei contenuti e dei servizi, anche laddove un *under* 13 tra i 9 e i 12 anni menta, il divario cognitivo non sia incolmabile tanto quanto quello tra un sedicenne e un minore di età compresa tra i 9 e i 13 anni;

Queste le ragioni per cui, ancora una volta, si auspica la riduzione a 13 anni dell'età affinché il consenso del minore, autonomamente conferito, venga considerato valido.

3.2 E se la sicurezza *online* diminuisse all'aumentare dell'età del consenso?

Pur prendendo per valido ciò che finora è stato illustrato, è indubbio che, a prima vista, si potrebbe affermare che l'aumento dell'età per la validità del consenso digitale sia in grado di determinare, almeno in via generale, una maggiore sicurezza dei minori: meno accedono alla rete tra i 13 e i 15 anni, più il genitore viene coinvolto nella scelta del conferimento dei dati degli *under* 16, maggiore sarà la protezione dei giovanissimi dai rischi del web. Peccato che la luna, per quanto luminosa possa apparire, possiede pur sempre un lato oscuro. E se innalzare l'età del consenso autonomo del minore contribuisse, invece, a far diminuire i livelli di sicurezza (sia come *safety*, sia come *security*) adottate dai fornitori dei servizi della società dell'informazione? È sempre Janice Richardson a sollevare una questione sul punto sostenendo, durante il dibattito sulla modifica dell'art. 8 RGPD, che spostare i requisiti per il consenso dei genitori dai 13 ai 16 anni rischia di deprivare i ragazzi di opportunità educative e sociali in molti modi, senza fornire più protezione, ma forse addirittura diminuendola[21].
In effetti, determinare una nuova soglia d'età per la validità del consenso digitale implica che i fornitori di servizi *online* ovviamente 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

[21] "*As experts working for the safety and wellbeing of children online, we feel that moving the requirement for parental consent from age 13 to age 16 would deprive young people of educational and social opportunities in a number of ways, yet would provide no more (and likely even less) protection*", in https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.s0ms9s15i.

di sistemi di verifica del consenso genitoriale (cfr. paragrafo 4). 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. 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 (cfr. paragrafo 3.2) rende molto difficile per i fornitori di servizi offrire contenuti e strumenti idonei. Così verrebbe meno non solo la libertà di accesso, di espressione, di associazione dei ragazzi tra i 13 e i 15 anni (cfr. paragrafo 4.1), ma anche la possibilità di aiutarli a vivere un'esperienza *online* sicura e *privacy-friendly*, senza dover assumere un'altra identità – quantomeno anagrafica.

In sintesi:

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?
Per rispondere a questa domanda, sono state prese in esame diverse conseguenze che un'età minima troppo elevata comporterebbe:

- Impatti dal punto di vista educativo. Nel report redatto alla fine del 2014 da Net Children Go Mobile 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**. Tenere alta l'età del consenso digitale autonomo non aiuterebbe a prevenire i rischi, lo dicono anche le associazioni europee impegnate nella tutela dei minori: tra i 13 e i 15 anni i giovani sentono già l'esigenza di ragionare, dibattere e decidere – in virtù del cd. "pensiero complesso" – e, per questo, tenderanno volersi connettere e ad aggirare i meccanismi e le *policy* che escludono i minori di 16 anni dai servizi *online*. Se tutti i ragazzi al di sotto dei 16 anni dovessero chiedere il permesso ai genitori per utilizzare con un proprio *account* i servizi *online* ne risentirebbero molte attività scolastiche, le ricerche, lo sviluppo di capacità critiche e di selezione delle informazioni, ma soprattutto si indebolirebbe lo stesso processo formativo che avviene – esso stesso – tramite l'uso di servizi web.
È, inoltre, completamente assente un programma di formazione incluso nella didattica a discapito delle conclusioni degli studi di EU Kids Online e dell'European Schoolnet, i quali evidenziano che più i ragazzi usano Internet, più acquisiscono competenze digitali e che nella fascia di età compresa tra i 12 e i 17 anni sono molto più consapevoli degli adulti rispetto a quali informazioni dovrebbero essere condivise *online*.

Gli studenti europei sprovvisti di una legge nazionale che porti a 13 anni l'età del consenso digitale sarebbero fortemente svantaggiati, sul piano educativo e culturale, rispetto ai loro coetanei americani o australiani e si creerebbe un **"*digital divide* europeo"** in termini di accesso alle risorse della rete.

- Impatti dal punto di vista delle dinamiche sociali dei minori. Come evidenziato da EU Kids Online e dall'European Schoolnet, gli *under* 13 già mentono sulla loro età pur di accedere ai servizi online e, 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. Il tipo di incoraggiamento che gli adolescenti riceverebbero dalla fissazione dell'età minima a 16 anni sarebbe quello di **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. 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.

- Impatti sull'offerta dei contenuti. **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.

- Impatti sulla sicurezza dei minori in rete. 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**.

4. Ulteriori considerazioni di carattere giuridico: perché i 13 anni favoriscono la tutela dei minori e la *compliance* aziendale

A seguito dell'analisi sulle possibili conseguenze sociali e culturali della fissazione "anziana" dell'età per il consenso digitale *ex* art. 8.1 (cfr. paragrafo 3), mettendo insieme alcuni degli elementi già evidenziati precedentemente, si proverà a descrivere in che modo una legge nazionale che porti la suddetta età a 13 anni sia preferibile da un punto di vista giuridico, sia con riferimento ai diritti e alla tutela dei minori, sia per quanto riguarda la regolazione relativa ai fornitori di servizi della società dell'informazione e la *compliance* degli stessi.

4.1 Rispetto dei diritti dei minori e della loro sfera personale: la tutela passa anche da qui

Nel paragrafo 2 è stata introdotta la questione relativa ai **diritti dei minori rispetto all'accesso e all'uso del web**. La CDIA ha fornito le basi per comprendere in che termini "*il fanciullo*" abbia "*diritto alla libertà di espressione*" (art. 13.1) inteso come "*la **libertà di ricercare, di ricevere e di divulgare informazioni e idee** di ogni specie, indipendentemente dalle frontiere, sotto forma orale, scritta, stampata o artistica, **o con ogni altro mezzo a scelta del fanciullo***". L'art. 12.1, invece, gli garantisce "*il **diritto di esprimere liberamente la sua opinione** su ogni questione che lo interessa*". In parallelo, l'art. 14, sancisce il diritto "*alla **libertà di pensiero, di coscienza e di religione***" e l'art. 15, quello "*alla **libertà di associazione** e alla **libertà di riunirsi pacificamente***".

Usare i social network o le piattaforme *online* e aderire alle *community* non è forse un modo per esercitare la libertà di ricercare, ricevere e divulgare informazioni e idee, esprimendo liberamente la propria opinione in termini di pensiero, coscienza e religione nonché di associarsi e riunirsi pacificamente?

Privare dell'accesso autonomo ai *social media* i ragazzi di età compresa tra i 13 e i 15 anni significa ledere non solo i loro diritti nel mondo digitale, ma anche impedire loro di partecipare a impegni di diversa natura (es. scolastici, civici, culturali, associativi ecc.). A tal proposito, in una recente pubblicazione del Consiglio d'Europa[22], viene evidenziato che, ferma restando la necessità di guida e di protezione nell'uso di internet, bambini e ragazzi[23] hanno:

- il diritto e la libertà di esprimere i propri punti di vista liberamente e di essere coinvolti nella società;
- la facoltà di aspettarsi di ricevere un'istruzione, a scuola e in famiglia, circa l'uso sicuro della rete e della protezione della privacy;
- il diritto a ricevere una protezione speciale *online* rispetto al benessere fisico, mentale e morale, con particolare riferimento allo sfruttamento sessuale e all'abuso, ma anche dalle altre forme di *cybercrime*. In particolare, questo diritto può essere applicato laddove venga rispettato anche quello ad essere educato a proteggersi dalle suddette minacce;

[22] http://www.coe.int/en/web/internet-users-rights/children-and-young-people.
[23] Secondo la Raccomandazione CM/Rec(2012)2 del Consiglio d'Europa, si considerano "bambini e ragazzi" tutti coloro che hanno un età inferiore ai 18 anni, in https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cb0ca#_ftn2.

- il dovere di rendersi conto che i contenuti creati *online* possono essere accessibili il tutto il mondo e compromettere la dignità, la sicurezza e la privacy sia nell'immediato sia una volta raggiunta la maggiore età. Ecco perché l'art. 17.1.f), riguardante il diritto alla cancellazione dei propri dati, in combinato disposto con il Considerando 65, dà peso e legittimità all'oblio qualora l'interessato abbia prestato il proprio consenso "*quando era minore, e quindi* ***non pienamente consapevole dei rischi*** *derivanti dal trattamento*";
- il diritto di ricevere informazioni chiare circa i comportamenti e i contenuti illeciti sul web così come di avere la possibilità di segnalarli confidenzialmente e anonimamente, in modo agevole per tutte le età.

In virtù degli standard stabiliti dal Comitato dei Ministri[24], il Consiglio d'Europa chiarisce, con apposito Memorandum[25], che **il diritto di bambini e ragazzi a partecipare si applica integralmente all'ambiente della rete**. Quest'ultima, infatti, costituisce per molti adolescenti la risorsa mediante cui ottenere notizie sugli avvenimenti correnti e mantenersi informati rispetto alla società in cui vivono.
Sono diverse, dunque, le fonti del diritto che avallano la tesi secondo cui il mancato passaggio dai 16 ai 13 anni finirebbe per determinare una mutilazione di importanti diritti riconosciuti ai minori e, in particolare, la citata Raccomandazione del Consiglio d'Europa pone l'accento sulla necessità di educare a un uso sicuro della rete. Peraltro, la stessa Unione Europea, nel suo sito dedicato a ragazzi tra i 13 e i 18 anni, sottolinea che "*Il cyberspazio è un mondo virtuale che offre molte opportunità: è possibile partecipare a social network e blog, giocare, imparare e fare tante altre cose.* ***Pur non essendovi motivo di non avvalersi di queste possibilità, occorre essere consapevoli dei rischi*** *che presentano, che non sono affatto virtuali, ed essere preparati ad affrontarli*"[26]. Ed è sempre dell'Unione Europea l'istituzione del programma "Better Internet for Kids"[27] (fino al 2013 intitolato "Safer Internet") che, tra gli altri, ha l'obiettivo di promuovere non solo l'educazione all'uso della rete e la classificazione dei contenuti, ma anche di creare un ambiente *online* più sicuro attraverso l'attuazione di iniziative di autoregolamentazione[28] tra le parti interessate (di cui si dirà meglio nel paragrafo 4.2).

Quando si parla dei diritti "digitali" dei minori, non bisogna trascurare il fatto che **l'accesso ai servizi web non è solo un diritto per esercitare altri diritti** (libertà di ricercare, ricevere e divulgare informazioni e idee, esprimere liberamente la propria opinione in termini di pensiero, coscienza e religione, associarsi e riunirsi pacificamente) **ma è anche lo strumento mediante il quale alcuni diritti possono essere tutelati** laddove vi sia una violazione reale o presunta, oppure qualora vi sia un disagio sociale connesso all'esercizio delle libertà del minore. Per questa ragione, il Considerando 38 del RGPD precisa, fra l'altro, che: "*Il consenso del titolare della*

[24] Ibid.
[25] http://www.coe.int/en/web/internet-users-rights/children-and-young-people-explanatory-memo.
[26] https://ec.europa.eu/0-18/wrc_index_en.jsp?main=true&initLang=IT.
[27] COM/2012/0196, in http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52012DC0196&from=EN.
[28] https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids.

responsabilità genitoriale non dovrebbe essere necessario nel quadro dei ***servizi di prevenzione o di consulenza forniti direttamente a un minore***".

La questione del consenso genitoriale per gli *under* 16, a ben guardare, pone un problema in quanto il consenso diventa per l'adulto un'incombenza, ma non tutti i genitori agiscono nel miglior interesse dei propri figli (ad es. in caso di abusi domestici).

Internet è sempre stato, soprattutto per i ragazzi dai 13 anni in su, uno strumento per far sentire la propria voce o affrontare delle difficoltà (discriminazione, bullismo, abusi, emarginazione sociale ecc.).

Ciò è però avvenuto non soltanto grazie ai servizi di cui al Considerando 38, ma anche e soprattutto mediante l'uso dei social e/o di *community* non "istituzionali", non finalizzate, cioè, alla prevenzione e alla consulenza diretta ai minori. Questi strumenti non hanno necessariamente un fine assistenziale ma, nonostante ciò, sono di grande supporto e aiuto per il ripristino dei diritti e della dignità dei più giovani che vivono situazioni di disagio fisico o mentale. Si pensi ai gruppi Facebook LGBTQ o alle pagine che nascono per sostenere le giovani vittime di crimini e abusi, ai forum in cui si discute di sessualità, di bullismo, ma anche ai *trend topic* di solidarietà, creati proprio dai ragazzi, mediante *hashtag* su Twitter o ai contenuti che essi caricano su piattaforme come YouTube per sensibilizzare, responsabilizzare e aiutare coetanei e non.

Impedendo ai ragazzi tra i 13 e i 15 anni di partecipare, il ***digital divide*** di cui al paragrafo 3.1, relativo all'accesso alle risorse, non sarebbe più inerente solo all'impossibilità di formarsi intellettualmente dal punto di vista didattico o educativo, ma anche all'**esclusione dagli strumenti che hanno utilità sociale**.

La burocratizzazione del meccanismo di consenso tra i 13 e i 15 anni potrebbe restringere drasticamente il raggio di azione dei minori nel senso di cui sopra, arrivando anche a erodere la privacy dei ragazzi stessi, che dovrebbero ottenere il consenso dei genitori per esercitare in modo "non istituzionale" (servizi di prevenzione e consulenza dedicata) i propri diritti e le proprie libertà.

Malala Yousafzai, la più giovane Premio Nobel per la pace in virtù del suo impegno per l'affermazione dei diritti civili e per il diritto all'istruzione, è la testimonianza della necessità di utilizzare le piattaforme del web anche per fini non-convenzionali, ma fondamentali. Durante il discorso tenuto a New York il 12 luglio del 2013, nell'Headquarter dell'ONU[29], alla ragazza è stata posta la seguente domanda: "*Cosa consiglieresti a qualcuno che crede che stia avvenendo un'ingiustizia nella sua comunità ma che non sa come iniziare a produrre un impatto concreto per rimuoverla?*". Yousafzai ha risposto così: "*Penso che sia facile. È pieno di persone che inizierebbero domandandosi 'Chi devo incontrare per dire cosa sta succedendo? Dove devo andare per farlo?'. Ma lo strumento di fronte a voi sono i social media. Usateli.* […] *È difficile alzarsi e dire a un talebano che ciò che sta facendo è sbagliato, se questi è di fronte a te nella tua casa. È più facile dar vita a una protesta pacifica su Facebook*". Ebbene, l'insegnamento della giovane ragazza pakistana è applicabile anche all'uso dei *social media* e dei servizi web da parte dei minori: **non tutti sono nella posizione di chiedere il consenso ai propri genitori, non**

[29] https://www.facebook.com/Pakistan.Malala/posts/739980896050369:0.

tutti lo otterrebbero, eppure spesso il primo passo per rimuovere le ingiustizie fisiche e mentali è la creazione di un profilo social o l'adesione a uno spazio virtuale in cui poter manifestare la propria opinione liberamente, liberamente in termini di diritto a esprimersi ma anche di farlo privatamente e autonomamente, senza che vi siano interferenze genitoriali nella sfera personale. Dopotutto, la privacy è anche questo.

4.2 Autoregolamentazione e codici di condotta a tutela dei minori: la nuova frontiera della *compliance*

Si è riflettuto, nel paragrafo 3.2, sulla necessità di adeguare i contenuti in base alle diverse fasce di età cui appartengono gli utenti sotto i 18 anni. Nel paragrafo 3.3, quindi, si è precisato che, per garantire ai minori una maggiore sicurezza *online*, è necessario anche mettere in condizione le imprese del settore ICT di sentirsi responsabili socialmente affinché esse implementino *best practices* e strumenti che tutelino i più piccoli.
Nel paragrafo 4.1, invece, si è fatto riferimento all'istituzione, da parte dell'Unione Europea, del programma "Safer Internet", oggi "Better Internet for Kids"[30] che ha l'obiettivo di promuovere un ambiente *online* più sicuro attraverso l'attuazione di iniziative di **autoregolamentazione**[31] tra le parti interessate. E in effetti, assieme alla questione dei contenuti e delle *best practices*, 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.

A tale scopo, preme sottolineare la disponibilità di due risorse:

- la prima è costituita dall'**Alliance to better protect minors online**. Si tratta di un'iniziativa di autoregolamentazione il cui fine è migliorare l'ambiente *online* per i ragazzi. Le maggiori compagnie ICT e media[32], insieme a diverse ONG[33] e all'UNICEF, hanno ufficialmente presentato l'Alleanza durante il Safer Internet Day 2017[34] le cui strategie sono sostanzialmente tre: 1) lo *user-empowerment* che includa strumenti per i genitori, classificazione dei contenuti e altri *tool* per la sicurezza online dei ragazzi (ad es. meccanismi di segnalazione più *user-friendly* e feedback di risposta); 2) l'impegno da parte degli operatori aderenti a intensificare la cooperazione e lo scambio di buone pratiche, tenendo conto degli input delle ONG, della società civile, delle autorità europee e nazionali e delle organizzazioni internazionali; 3) il favorire l'aumento, da parte di tutti i membri dell'Alleanza, della consapevolezza degli utenti minorenni, promuovendo l'accesso a contenuti positivi, educativi e diversificati.

[30] https://ec.europa.eu/digital-single-market/safer-internet-better-internet-kids.
[31] https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids.
[32] ASKfm, BT Group, Deutsche Telekom, Facebook, Google, KPN, The LEGO Group, Liberty Global, Microsoft, Orange, Rovio, Samsung Electronics, Sky, Spotify, Super RTL, TIM (Telecom Italia), Telefónica, Telenor, Telia Company, Twitter, Vivendi, Vodafone.
[33] BBFC, Child Helpline International, COFACE, eNACSO, EUN Partnership, FOSI, FSN, GSMA, ICT Coalition, NICAM, Toy Industries of Europe, UNICEF.
[34] https://ec.europa.eu/digital-single-market/en/news/safer-internet-day-2017-european-commission-welcomes-alliance-industry-and-ngos-better-internet.

- La seconda risorsa è costituita dai **codici di condotta**, introdotti con il RGPD *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 ulteriore verso l'***enforcement*** **delle buone pratiche** che non hanno di per sé natura obbligatoria. La stessa Alleanza si basa sull'impegno volontario degli aderenti. Il Considerando 77 del RGPD precisa invece 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, impegni quali quelli previsti dall'Alleanza o gli altri emersi come auspicabili nel corso di questo breve *paper* diventerebbero vincolanti per i titolari e i responsabili del trattamento al fine di ottemperare alle disposizioni del codice stesso e, quindi, del RGPD.

Mantenendo aperta la questione dei "codici di condotta", è necessario tornare per un istante all'art. 8.1 RGPD. "*Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni*": **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)[35], 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* 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 (cfr. paragrafo 3.2) oppure, 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*. Insomma, il ***digital divide*** di cui si è parlato più volte con riferimento all'accesso a risorse didattiche, educative o di utilità sociale, andrebbe a estendersi anche alla gamma di servizi per le più varie attività digitali: mandare e-mail, caricare foto su Instagram o video su YouTube, giocare *online*, accedere a contenuti *on demand*, fare acquisti ecc.

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

[35] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children%27s-privacy.

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 RGPD 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 RGPD.

Sembra, insomma, che non solo a livello internazionale, ma soprattutto in sede europea, ci si stia muovendo in una direzione che tende a favorire l'inclusione dei più giovani sulla rete, non la loro esclusione, tutelandoli con diversi strumenti, molti dei quali auspicati anche nel presente lavoro.

In definitiva, **l'adozione di una legge nazionale che riduca la soglia anagrafica del consenso digitale a 13 anni sembra essere perfettamente in linea con gli stessi obiettivi dell'UE, con i suoi principi e con i diritti e libertà fondamentali da essa riconosciuti agli individui di ogni età. In Italia, la strada percorribile potrebbe consistere nella previsione di un articolo *ad hoc* della legge di delegazione europea 2017 o 2018, in grado di conferire al Governo il potere di intervenire in materia con serietà, eventualmente anche prevedendo ulteriori cautele a salvaguardia degli *under-16* con riferimento, per esempio, alla chiarezza e comprensibilità dell'informativa.**

In sintesi:

- Usare i social network o le piattaforme *online* e aderire alle *community* è un modo per esercitare la libertà di ricercare, ricevere e divulgare informazioni e idee, esprimendo liberamente la propria opinione in termini di pensiero, coscienza e religione nonché di associarsi e riunirsi pacificamente. Privare dell'accesso autonomo ai *social media* i ragazzi di età compresa tra i 13 e i 15 anni significa ledere i loro diritti nel mondo digitale e impedirgli di partecipare a impegni di diversa natura (es. scolastici, civici, culturali, associativi ecc.), contrariamente a quanto previsto dalla Convenzione sui diritti dell'infanzia e dell'adolescenza e dal Memorandum del Consiglio d'Europa in cui viene dichiarato che **il diritto di bambini e ragazzi a partecipare si applica integralmente all'ambiente della rete**.

- La questione del consenso genitoriale per gli *under* 16 pone un problema in quanto il consenso diventa per l'adulto un'incombenza, ma non tutti i genitori agiscono nel miglior interesse dei propri figli (ad es. in caso di abusi domestici). Quando si parla dei diritti "digitali" dei minori, **l'accesso ai servizi web non è solo un diritto per esercitare altri diritti** (libertà di ricercare, ricevere e divulgare informazioni e idee, associarsi ecc.) **ma è anche lo strumento mediante il quale alcuni diritti possono essere tutelati** laddove vi sia una violazione reale o presunta, oppure qualora vi sia un disagio sociale connesso all'esercizio delle libertà del minore. Per questa ragione, il Considerando 38 del RGPD precisa che: "*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***". Tuttavia i servizi di cui al Considerando 38 non sono gli unici ad essere funzionali alla tutela dei diritti del minore, giacché essa avviene soprattutto mediante l'uso dei social e/o di *community* non finalizzate esplicitamente alla prevenzione e alla consulenza diretta ai minori.

Spesso il primo passo per rimuovere le ingiustizie fisiche e mentali è la creazione di un profilo social o l'adesione a uno spazio virtuale in cui poter manifestare la propria opinione liberamente, liberamente in termini di diritto a esprimersi ma anche di farlo privatamente e autonomamente, senza che vi siano interferenze genitoriali nella sfera personale.

Impedendo ai ragazzi tra i 13 e i 15 anni di partecipare, il ***digital divide*** consisterebbe anche nell'**esclusione dagli strumenti che hanno utilità sociale per far ascoltare la propria voce o affrontare delle difficoltà** (discriminazione, bullismo, abusi, emarginazione sociale ecc.).

- **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), l'età del consenso digitale è fissata a 13 anni. I *service provider* potrebbero reagire in due modi: decidendo 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; oppure, 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*. Il ***digital divide europeo*** andrebbe a estendersi anche alla gamma di servizi per le più varie attività digitali (mandare e-mail, caricare foto o video sulle piattaforme di *sharing*, giocare *online*, accedere a contenuti *on demand*, fare acquisti ecc.).

In definitiva, **l'adozione di una legge che riduca la soglia anagrafica del consenso digitale a 13 anni sembra essere perfettamente in linea con gli stessi obiettivi dell'UE, con i suoi principi e con i diritti e libertà fondamentali da essa riconosciuti agli individui di ogni età**.

5. Un'appendice per riflettere, con le parole dell'Autorità italiana

Per continuare a riflettere su quanto affermato nel corso di questo *paper*, si riporta la dichiarazione di Antonello Soro, Presidente del Garante italiano per la Protezione dei Dati Personali, a margine del suo intervento durante il convegno "Insieme per un web più sicuro (*Be The Change: United For A Better Internet*)" tenutosi a Roma nel giorno del Safer Internet Day 2017:

"[…] *Che fare? Come* ***conciliare libertà e responsabilità in rete****? È, questo, un tema che interroga le classi dirigenti in ogni angolo del pianeta. E non esistono soluzioni miracolistiche.*

Non è scontato né banale richiamare intanto quel controllo parentale che mai deve essere considerato residuale: il modo migliore per tutelare i ragazzi dalle insidie del web, è rafforzare la loro ***consapevolezza*** *rispetto alle implicazioni che ha ogni parola, immagine o altra espressione in rete e investire sull'educazione digitale quale vera e propria "educazione civica" al tempo della cittadinanza digitale.*

Così come sarà indispensabile ***promuovere e rafforzare una solida alleanza educativa tra scuola e famiglia****. È questa la prima e più importante frontiera su cui tutti dobbiamo investire. Ma per fronteggiare uno scenario così articolato, dove l'uso interattivo delle nuove forme di comunicazione rende estremamente difficile proteggere i minori da loro stessi e da ogni possibile fenomeno illecito, è necessaria una decisa strategia di risposta sia da parte di tutte le istituzioni pubbliche che degli operatori privati.*

Sicuramente un ruolo incisivo possono assumere i gestori delle piattaforme tecnologiche, in modo da minimizzare (in un'ottica davvero di ***riduzione del danno****) gli effetti prodotti dalla presenza e dalla persistenza in rete di espressioni violente, ingiuriose, diffamatorie nei confronti di minori, secondo modalità già sperimentate con riferimento alla pedopornografia, all'istigazione all'odio e, più recentemente, alla prevenzione dei fenomeni di radicalizzazione online.*

[…]

Negli ultimi tempi viene riproposto il bisogno di regole capaci di rendere inaccessibili alcuni siti ai minori. In generale temo che ***l'idea di fissare una soglia di età nel mondo digitale per proteggere i minori dai pericoli della rete rischi di essere una soluzione puramente convenzionale****: non solo per la difficoltà di stabilire presuntivamente una rigida correlazione tra età e consapevolezza digitale, ma soprattutto per la* ***facilità di eludere simili criteri di accesso****.*

[…]

Maggiori criticità emergono rispetto a metodi di accertamento documentale dell'età, certamente più efficaci, ma che implicherebbero, se generalizzati, una ***raccolta di dati massiva****, peraltro in un contesto in cui, al contrario, essa dovrebbe essere ridotta al minimo necessario. L'idea di poter rendere il web un'area ad accesso "limitato", cui concedere l'ingresso ai soli maggiorenni provandone l'età con un documento di identità si tradurrebbe quindi in una* ***schedatura di massa****.*

Schedatura peraltro effettuata da soggetti privati che finirebbero per aumentare ulteriormente il loro potere, detenendo una sorta di ***anagrafe della popolazione mondiale****, in palese controtendenza rispetto alla filosofia che permea il nuovo Regolamento europeo in materia di protezione dati.*

E, infine, vorrei ricordare che, come in tutte le strategie proibizioniste, ***il rischio ulteriore consiste nel fatto che all'oggetto proibito si acceda comunque per altra via, o eludendo i controlli con furti di identità o muovendosi nel ben più pericoloso deep web, dove le insidie sono di certo maggiori***".

www.istitutoprivacy.it

www.anticyberbullismo.it

Roma, 7 marzo 2017