

## Minori e social media: tutela dei dati personali, autoregolamentazione e privacy

GIORGIO PEDRAZZI\*

SOMMARIO: 1. *Minori e social media* – 2. *Privacy e servizi della società dell'informazione per i minori* – 3. *La tutela dei minori nel GDPR* – 3.1. *Età del consenso* – 3.2. *Informativa* – 3.3. *Diritto all'oblio* – 3.4. *Codici di condotta, vigilanza e autoregolamentazione*

### 1. MINORI E SOCIAL MEDIA

Da sempre la comunità svolge un ruolo importante nella formazione dell'individuo nel processo che porta dall'infanzia verso l'età adulta. Al giorno d'oggi il minore ha a disposizione numerosi ambiti e strumenti per esprimere e forgiare la sua personalità ed esercitare i diritti a lui riconosciuti dalle convenzioni internazionali, anche attraverso l'utilizzo di tecnologie in grado di permettere nuovi modelli di relazione. L'avvento dei c.d. social media<sup>1</sup> ha, infatti, determinato una rivoluzione nelle modalità di interazione e comunicazione personale, introducendo anche profonde ricadute sulle attività commerciali e negoziali. Dal punto di vista tecnologico si tratta di strumenti e piattaforme costantemente oggetto di ricerca e sviluppo, dei veri laboratori in mutamento per mantenere l'attrattività e ottenere un coinvolgimento sempre più intenso dell'utilizzatore.

Tutto questo fermento ha l'obiettivo di catturare la costante attenzione<sup>2</sup> e l'attività di un numero sempre maggiore di utenti, volenterosi a collaborare, a garantire così la continua crescita di tali strumenti e allontanare i competitor, che peraltro s'inseriscono in un quadro mutevole di fusioni e acquisizioni.

Per ottenere risultati sempre più stupefacenti da fornire al mercato degli investitori e degli operatori che acquistano gli spazi pubblicitari on line, lo sviluppo tecnologico continua incessantemente a fornire e rinnovare applicazioni

\* L'A. è professore aggregato di Istituzioni di diritto privato presso l'Università degli Studi di Brescia.

<sup>1</sup> Per un *excursus* storico vedi J. VAN DIJCK, *The Culture of Connectivity: A Critical History of Social Media*, Oxford, Oxford University Press, 2013, *passim*.

<sup>2</sup> Sull'attenzione come obiettivo dei gestori dei servizi on line vedi la lucida analisi di T. WU, *The Attention Merchants: The Epic Scramble To Get Inside Our Heads*, New York, Alfred A. Knopf, 2016.

oltre a integrare gli elementi esistenti. Questo processo si traduce inevitabilmente in una maggiore concentrazione delle informazioni con conseguente esposizione a rischi più elevati per la sicurezza e la privacy degli utenti.

La continua ed esasperata corsa all'innovazione produce un aumento della complessità che richiede infrastrutture più solide sotto il profilo della sicurezza e introduce conseguentemente un incremento di rischi, nuove criticità che possono esporre a vulnerabilità i dati e le informazioni degli utenti, rendendo più ardua la tutela giuridica dei soggetti coinvolti.

La natura stessa dei social media favorisce l'integrazione tra gli stessi, come per il caso di social network propriamente detti e sistemi di *instant messaging*, oggetto di convergenza tra le corporation<sup>3</sup>.

Nel caso dei minori, ad esempio, destano preoccupazione gli sviluppi legati a un uso indiscriminato e poco avveduto di apparecchi wearable legati all'Internet of Things (IoT) come nel caso di giocattoli interattivi, specificamente destinati ai bambini, ma anche di smartwatch, sempre più spesso utilizzati da soggetti giovanissimi<sup>4</sup>.

Nel contesto della presente indagine, cercheremo di affrontare la questione specifica delle interazioni dei minori sui social media e dell'impatto in termini di riservatezza e protezione dei dati personali di queste attività. Preliminarmente è opportuno tratteggiare i confini degli strumenti oggetto di analisi. Pur in un quadro tecnologico anch'esso in evoluzione, è possibile identificare alcuni processi diffusi che costituiscono i tratti identificativi del fenomeno social media in quanto tale<sup>5</sup>. In uno studio del 2015<sup>6</sup>, ad esempio, sono stati individuati i seguenti caratteri comuni ai social media:

<sup>3</sup> Il riferimento corre all'acquisto del sistema di IM Whatsapp da parte del colosso Facebook. Sulle modalità di flusso intragruppo dei dati personali degli utenti è in corso un'indagine delle autorità di controllo dell'Unione europea che fa seguito alla sanzione di 110 milioni di euro irrogata a Facebook nel maggio 2017 da parte della Commissione Ue anche per grave violazione della norma in materia di concorrenza. I garanti privacy di Francia e Germania hanno già intimato di non condividere i dati tra le due società.

<sup>4</sup> Vedi il report NORWEGIAN CONSUMER COUNCIL (NCC), *#WatchOut Analysis of Smartwatches for Children*, <https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf>, October 2017.

<sup>5</sup> In generale sui profili giuridici cfr. R. CAFARI PANICO, *Da Internet ai social media*, Santarcangelo di Romagna, Maggioli, 2013.

<sup>6</sup> J.A. OBAR, S. WILDMAN, *Social Media Definition and the Governance Challenge: An Introduction to the Special Issue*, in "Telecommunications Policy", vol. 39, 2015, n. 9, pp. 745-750.

- a) l'utilizzo generalizzato, almeno allo stato presente, della tecnologia del web 2.0;
- b) il massiccio assorbimento di UGC - *User-Generated Content*;
- c) la profilazione degli utenti del sito o della app;
- d) la connessione dei profili con quelli di altri utenti o gruppi di utenti.

Tutti questi elementi, favorendo una coinvolgente esperienza dell'utente, offrono modalità di utilizzo particolarmente efficaci nel presentare possibilità enormi di relazione, ma al tempo stesso sicuramente prospettano anche per-spicui rischi per la privacy e per l'autonomia negoziale degli utenti in generale e ancora più gravi per i minori. La distinzione sulla base dell'età anagrafica degli utenti discende da considerazioni empiriche largamente condivise. Se infatti l'impatto nel breve termine è stato decisamente più traumatico per gli individui già maturi e inseriti in un modello di comunicazione legato ai media tradizionali, questi stessi soggetti si sono comunque ritrovati a subire una forzata interazione con i nuovi strumenti. Molto spesso ciò si è tradotto in una sorta di delega generica ai propri figli per la gestione delle questioni tecnologiche familiari, processo che implica una sostanziale legittimazione dei minori a operare liberamente nella Rete anche per attività negoziali non direttamente affidate dai genitori stessi.

La progressiva semplificazione dei processi e un progressivo incremento nell'alfabetizzazione informatica hanno permesso un graduale ribilanciamento dei ruoli e una maggiore comprensione dell'importanza delle attività che si compiono in Rete.

La fallacia dell'equazione che traduce la padronanza dello strumento con la consapevolezza delle conseguenze delle azioni connesse e le contestabili categorizzazioni dei "nativi digitali" o "millennials" ha talvolta condotto ad una sottovalutazione dei pericoli e dei rischi connessi all'uso degli strumenti.

Il quadro normativo della tutela dei minori sui media, per quanto articolato, non sembra mai sufficiente a proteggere in modo efficace i bambini che svolgono sempre maggiore e diversificata attività in Rete. La tutela dei minori nell'utilizzo dei servizi della società dell'informazione assume oggi una rilevanza strategica anche perché sono maggiormente esposti a subire, per lungo tempo, le conseguenze dell'attività on line propria o di soggetti ad essi collegati.

La *datification* e la connettività semplificano le nostre attività quotidiane ma, al tempo stesso, producono conseguenze talora indesiderate<sup>7</sup>. Come già

<sup>7</sup> D. LUPTON, B. WILLIAMSON, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, in "New Media & Society", vol. 19, 2017, n. 5, pp. 780-794.

precisato, i rischi sono connessi alla sicurezza e alla tutela della privacy e dei dati personali relativi a tutti gli individui, ma l'impatto sarà differenzialmente maggiore sulla vita futura di un bambino<sup>8</sup>.

Per definire l'importanza è utile richiamare la nozione di *networked self*, cioè la proiezione virtuale della propria identità o di una molteplicità delle stesse. Essa, nel caso del minore, è generata in parte da quanto immesso direttamente dal singolo, in parte da quanto inserito da soggetti diversi ma collegati a quest'ultimo (tra questi i genitori, le scuole e gli enti governativi e, infine, amici e conoscenti)<sup>9</sup>.

L'immissione di contenuti da parte dei genitori costituisce sempre più oggetto di aspro dibattito a diversi livelli, giungendo a lambire le aule giudiziarie<sup>10</sup>.

Un terzo soggetto è rappresentato dalle stesse piattaforme social, che utilizzano e manipolano i dati anche per scopi di profitto. Sullo sfondo, alcune di queste informazioni vengono analizzate da altri organismi pubblici e governativi per finalità di sorveglianza globale e sicurezza nazionale.

Per meglio comprendere le proporzioni del fenomeno, basti pensare che circa un quinto della popolazione dell'Unione europea è di età inferiore ai diciotto anni. La quota sale a un terzo se consideriamo la percentuale di minorenni in relazione al numero totale di naviganti europei della Rete.

In relazione all'adozione di idonei ed effettivi strumenti di tutela, è importante, in primo luogo, identificare la percezione dei minori stessi rispetto ai rischi connessi all'utilizzo di social media.

Sotto questo profilo, tra gli effetti perversi del cosiddetto *privacy paradox*, documentato nella letteratura sociologica, si ritrova la tendenza per i soggetti

<sup>8</sup> Sul tema vedi il recente studio di G. BERMAN. K. ALBRIGHT, *Children and the Data Cycle: Rights and Ethics in a Big Data World*, Innocenti Working Paper 2017-05, Florence, UNICEF Office of Research, 2017.

<sup>9</sup> K.C. MONTGOMERY, *Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications*, in "Telecommunications Policy", vol. 39, 2015, n. 9, pp. 771-786.

<sup>10</sup> Vedi lo scalpore destato da una recente sentenza di merito, secondo cui l'inserimento di foto dei figli minori sui social network avvenuto con l'opposizione di uno dei genitori integra violazione della norma di cui all'art. 10 c.c. (concernente la tutela dell'immagine), del combinato disposto degli artt. 4, 7, 8 e 145, d.lgs. 30 giugno 2003, n. 196 (riguardanti la tutela della riservatezza dei dati personali), nonché degli artt. 1 e 16, co. 1 e 2 della Convenzione di New York del 20 novembre 1989 ratificata dall'Italia con l. 27 maggio 1991, n. 176, sicché va vietata la pubblicazione di tali immagini e disposta la rimozione di quelle già inserite (Trib. Mantova, 19 settembre 2017). Si veda anche S. PERON, *Sul divieto di diffusione sui social network delle fotografie e di altri dati personali dei figli*, in "Responsabilità civile e previdenza", 2018, n. 2, p. 589.

più fragili e maggiormente esposti a conseguenze dannose a sottovalutare le controindicazioni e i pericoli in tema di privacy e a sottoutilizzare gli strumenti a disposizione<sup>11</sup>.

Le modalità di utilizzo dei social media da parte dei minori rendono spesso difficile il controllo da parte dei genitori, insegnanti ed educatori in genere. Ciononostante, tra i fattori in grado di incidere positivamente sulla consapevolezza dei minorenni resta fondamentale il ruolo degli insegnanti<sup>12</sup> e dei genitori<sup>13</sup> e l'emulazione di comportamenti positivi<sup>14</sup>.

In seconda battuta è necessario procedere con l'individuazione dei rischi concreti: numerose possono essere le conseguenze legate all'utilizzo di social media da parte di minori. Tra queste basti menzionare il problema dei furti di identità, che raramente vengono scoperti prima del diciottesimo anno, quando i danni reputazionali possono già aver assunto proporzioni gigantesche<sup>15</sup>. La pratica della *children online self exposure* può risultare dannosa per le future potenzialità lavorative, fino a incidere su profili più mirati come la possibilità di accedere a forme di credito (impatto sul *credit score*) o all'aumento dei costi di coperture assicurative.

<sup>11</sup> *Ex plurimis*, A. THIENE, *I diritti della personalità dei minori nello spazio virtuale*, in "Annali online della Didattica e della Formazione Docente", vol. 9, 2017, n. 13, pp. 26-39; A. SPANGARO, *Minori e mass media: vecchi e nuovi strumenti di tutela*, Milano, Ipsoa, 2011, *passim*; A. THIENE, *L'inconsistente tutela dei minori nel mondo digitale*, in "Studium iuris", 2012, n. 5, p. 528 ss.; C. PERLINGIERI, *La tutela dei minori di età nei social networks*, in "Rassegna di diritto civile", 2016, n. 4, p. 1324 ss.

<sup>12</sup> K. DAVIS, C. JAMES, *Tweens' Conceptions of Privacy Online: Implications for Educators, Learning, Media and Technology*, vol. 38, 2013, n. 1, pp. 4-25.

<sup>13</sup> Il ruolo dei genitori e il loro esempio resta fondamentale: S. YUSUF, M. NIZAM OSMAN, M. SALLEH HJ. HASSAN, M. TEIMOURY, *Parents' Influence on Children's Online Usage*, in "Procedia - Social and Behavioral Sciences", vol. 155, 2014, pp. 81-86, <https://doi.org/10.1016/j.sbspro.2014.10.260>; S. LIVINGSTONE, K. ÓLAFSSON, E. J. HELSPERD et al., *Maximizing Opportunities and Minimizing Risks for Children Online: The Role of Digital Skills in Emerging Strategies of Parental Mediation*, in "Journal of Communication", vol. 67, 2017, n. 1, pp. 82-105.

<sup>14</sup> Y. SEOUNMI, *Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach*, in "Journal of Broadcasting & Electronic Media", vol. 49, 2005, n. 1, pp. 86-110.

<sup>15</sup> D.C. VLADECK, *Consumer Protection in an Era of Big Data Analytics*, in "Federal Trade Commission, Child Identity Theft", <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>, 2012; ITRC - IDENTITY THEFT RESOURCE CENTER, *Fact Sheet 120: Identity Theft and Children*, <http://www.idtheftcenter.org/Fact-Sheets/fs-120.html>.

## 2. PRIVACY E SERVIZI DELLA SOCIETÀ DELL'INFORMAZIONE PER I MINORI

L'effettività degli strumenti giuridici per offrire garanzie al minore che naviga in Rete non è generalmente, allo stato attuale, considerata sufficiente a garantire un'elevata soglia di protezione<sup>16</sup>.

Il quadro giuridico offre una tutela multi-livello che muove dalle fonti di diritto internazionale arrivando alle iniziative dell'Unione europea. Dal punto di vista giurisdizionale, accanto all'*extrema ratio* del rimedio penale<sup>17</sup>, troviamo una disciplina civilistica incentrata sulla tutela dell'autonomia negoziale e della sicurezza della circolazione giuridica. Pare però sin d'ora evidente come in un settore in continua evoluzione debbano giocare un ruolo fondamentale gli strumenti di autoregolamentazione e la prassi delle autorità amministrative di controllo.

In una prospettiva globale, i risultati di uno studio patrocinato dall'UNICEF hanno evidenziato l'assenza di attenzione ai minori<sup>18</sup> da parte degli organismi della governance di Internet. Questa lacuna rappresenta sicuramente una questione di fondamentale importanza da affrontare attraverso un'interazione delle diverse fonti summenzionate. Il dialogo tra i diversi operatori sul tema è ancor più cruciale in considerazione della stessa natura sfuggente della Rete da un punto di vista istituzionale. Muovendo da un'analisi bottom-up degli strumenti a disposizione degli operatori del diritto per la tutela dei navigatori più giovani, il riferimento immediato è rappresentato dalla disciplina, di derivazione europea, riguardante la tutela della privacy. Per quanto il processo di costruzione di uno statuto europeo per la protezione dei dati personali risalga agli anni Novanta del secolo scorso, la questione oggetto del presente articolo è stata affrontata nello specifico soltanto in tempi recenti.

L'attenzione verso il trattamento dei dati dei minori rappresenta, infatti, una delle novità più importanti contenute nella nuova disciplina europea, convenzionalmente definita come GDPR - *General Data Protection Regulation*.

<sup>16</sup> J. ADAMOVIĆ, *Impact of General Data Protection Regulation on Children's Rights in Digital Environment*, in "Annals FLB - Belgrade Law Review", vol. 64, 2016, n. 3, p. 205.

<sup>17</sup> Vedi il caso *Vividown* e più in generale A. MONTI, *Tutela del minore, community on line e responsabilità penale del fornitore di servizi internet*, in "Cassazione penale", 2008, n. 2, p. 748.

<sup>18</sup> S. LIVINGSTONE, J. CARR, J. BYRNE, *One in Three: Internet Governance and Children's Rights*, Innocenti Discussion Paper No. 2016-01, Florence, UNICEF Office of Research, 2016.

Il nuovo pacchetto di protezione dei dati personali comprende una direttiva, rivolta alla disciplina del trattamento dei dati giudiziari, e un regolamento, oggetto specifico della presente analisi. Quest'ultimo dedica una specifica attenzione alla tutela dei minori, ma lo fa purtroppo con disposizioni che talora lasciano alcuni margini che potrebbero nuocere all'effettività della tutela.

Per quanto il considerando n. 7 sottolinei la necessità di certezza legale per garantire la protezione dei dati personali, una delle principali situazioni in grado di generare una potenziale incertezza è rappresentata precisamente dall'indicazione dell'età minima richiesta per l'accesso ai servizi da parte dei minori.

Anticipando alcune considerazioni che verranno rese nel prosieguo, va inoltre segnalato che non paiono sufficientemente definite le modalità con cui il consenso genitoriale andrebbe reso, non sono compiutamente affrontate la questione centrale che attiene all'ammissibilità e alle condizioni in base alle quali possa avvenire una profilazione dei minori e, infine, il requisito della trasparenza specificatamente richiesta in relazione ai rapporti con i bambini.

Com'è noto, la direttiva 46 del 1995, recepita prima dalla l. 31 dicembre 1996, n. 675<sup>19</sup> e poi confluita nel *Codice privacy* (d.lgs. 30 giugno 2003, n. 196), non operava una distinzione tra il trattamento di dati dei minori e quello di dati degli adulti. Nel corso della sua applicazione, però, il "Gruppo di lavoro art. 29" (*Working Party art. 29*)<sup>20</sup> in più occasioni aveva trovato modo di sottolineare l'esigenza di una cura particolare da prestare al trattamento dei dati di minori. Esplicitamente in tema di consenso, ma anche nel parere sugli apparecchi smart (la questione dei giocattoli è particolarmente rilevante), il *Working Party art. 29* sottolineava in particolare l'esigenza di evitare indebite influenze sui bambini, soggetti particolarmente esposti alle conseguenze negative di una pubblicità comportamentale o troppo mirata.

In generale, diversi documenti di provenienza Ue raccomandavano una maggiore attenzione sul punto<sup>21</sup>, pertanto la scelta della nuova disciplina si colloca in un solco già tracciato.

<sup>19</sup> L. SACCHETTI, *Privacy: nodi e scioglimenti con particolare riferimento alla tutela dei minori*, in "Famiglia e diritto", 1998, n. 3, p. 289.

<sup>20</sup> Il *Working Party art. 29* trae nome e funzione dalla norma della direttiva che lo ha istituito. Nel corso degli anni ha rappresentato un costante punto di riferimento e così anche nelle more dell'applicazione del GDPR. In un certo senso è il prodromo del nuovo *European board*.

<sup>21</sup> COMMISSIONE EUROPEA, *Strategia europea per un'internet migliore per i ragazzi*, doc. COM(2012) 196 del 2 maggio 2012; COMMISSIONE EUROPEA, *Programma UE per i diritti dei minori*, doc. COM(2011) 60 del 15 febbraio 2011 nei quali si definisce l'impegno delle istituzioni europee al raggiungimento degli standard richiesti dalle convenzioni internazionali e alla considerazione della prospettiva dell'interesse del minore.

Conseguentemente all'approccio basato sul rischio, il GDPR nel considerando n. 38, sottolinea il maggior rischio connesso al trattamento di dati personali dei minori.

Pur constatando l'attenzione riservata dal regolamento alla tutela dei fanciulli, si riscontra l'assenza di una espressa definizione di bambino, che viene tradizionalmente associata alla minore età. Sul punto precisamente il *Working Party*, nei suoi pareri resi precedentemente, considerava già una prospettiva statica e una dinamica di tutela, dicotomia della quale però non si trova traccia nel testo finale del GDPR.

Peraltro, la bozza di proposta di regolamento conteneva la definizione utilizzata dalla Convenzione UNCHR delle Nazioni unite, secondo la quale minorenne e bambino coincidono, a meno che questi non abbia già raggiunto la capacità di agire sulla base della legge nazionale.

Nel testo definitivo, i bambini, non meglio specificati, sono però identificati come «individui vulnerabili» meritevoli di «specifica tutela», secondo alcuni commentatori questa soluzione è però limitativa rispetto alla disciplina, quali soggetti titolari di diritti indipendenti di cui alla Convenzione UNCHR.

In relazione alla disciplina civilistica dell'autonomia privata dei minori va precisato che, coerentemente al regolamento di competenze dell'Unione, il testo dell'art. 8 del regolamento (UE) 2016/679 fa salva la disciplina degli Stati membri in ordine alla formazione e validità dei contratti<sup>22</sup>.

Premesse queste considerazioni in ordine all'ambito soggettivo, resta da approfondire il passaggio legato all'ambito oggettivo di applicazione, ovvero all'individuazione dei servizi a cui fa riferimento. Senza dubbio, i social media sono da considerarsi ricompresi a prescindere dalla richiesta di una qualsivoglia forma di pagamento di un corrispettivo, anche per mezzo dell'esposizione a forme di pubblicità. Resta in sospeso la questione se la disciplina si applichi anche ai dati raccolti on line inconsapevolmente dai provider, che soltanto successivamente si rivelino invece relativi a minori. Sotto questo profilo, secondo una prima interpretazione, offerta dall'autorità inglese ICO - *Information Commissioner's Office*, oggetto dell'art. 8 di cui sopra sarebbero soltanto i servizi rivolti esplicitamente ai minori. Sempre riguardo al profilo oggettivo si richiama la definizione di dati personali come PII - *Personal Identifiable Information* di cui al parere 4/2007 "on the concept of personal data" del Gruppo di lavoro art. 29.

<sup>22</sup> P. STANZIONE, *I contratti del minore*, in "Europa e diritto privato", 2014, n. 4, p. 1237; M. CINQUE, *Il minore contraente. Contesti e limiti della capacità*, Padova, Cedam, 2007.



In ogni caso, in estrema sintesi, il trattamento in oggetto concerne raccolta ed elaborazione dei dati personali che vedano interessato un minore identificato o identificabile, anche indirettamente, per servizi che siano attivabili on line tramite computer o smartphone<sup>23</sup>. Si tratta di servizi eterogenei, dall'attivazione di un account e-mail, all'iscrizione ad un social network o a una piattaforma di condivisione di contenuti multimediali, servizi cloud e molto altro ancora. Va sottolineato come la scuola oggi appaia sempre più digitalizzata e si stia ampliando l'offerta di strumenti e app in grado di supportare lo studente minorenni nello svolgimento delle sue attività scolastiche. L'argomento dei c.d. *learning analytics* sul fronte scolastico e la necessità di particolare attenzione da parte dei dirigenti degli enti formativi nella scelta e nell'adozione di strumenti informatici per la gestione dei dati personali degli studenti e delle carriere non andrà mai sufficientemente sottolineata.

Su un fronte più ampio, in relazione all'acquisto e alla fornitura di servizi on line, il minore costituisce un'allettante prospettiva di vendita per i provider. Nella prospettiva del minore-consumatore va menzionato che commercialmente i teenager vengono considerati come categoria di acquirenti sin dagli anni Quaranta del secolo scorso, mentre i *tween* vengono considerati tali negli anni Novanta<sup>24</sup>. I bambini hanno tre ruoli essenziali nel mercato: il mercato primario, mano a mano che ricevono dei soldi da poter spendere; il mercato genitoriale, come strumento di influenza sugli acquisti dei genitori; il mercato futuro, in quanto le abitudini assunte da piccoli condizioneranno le preferenze future<sup>25</sup>.

Con riguardo alle caratteristiche del minore, esso rileva oltre che sotto il profilo di consumatore anche come prosumer, per quanto l'eventuale attività di un minore come youtuber ecc. non fa perdere le tutele previste dal codice del consumo, ai sensi della definizione di consumatore sui social media.

<sup>23</sup> L. BOLOGNINI, C. BISTOLFI, *L'età del consenso digitale. Privacy e minori on line, riflessioni sugli impatti dell'art. 8 del Regolamento 2016/679(UE)*, [http://anticyberbullismo.it/wp-content/uploads/2017/06/Er%C3%A0\\_del\\_consenso\\_digitale\\_IIP\\_CNAC\\_2017.pdf](http://anticyberbullismo.it/wp-content/uploads/2017/06/Er%C3%A0_del_consenso_digitale_IIP_CNAC_2017.pdf), 7 marzo 2017.

<sup>24</sup> K.C. MONTGOMERY, *Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet*, Cambridge, The MIT Press, 2007. A. LAREKIA, J. ALTUNAB, J.I. MARTÍNEZ DE MORENTINC, N. AMENABARA, *Young People and Digital Services: Analysis of the Use, Rules, and Age Requirement*, in "Children and Youth Services Review", vol. 79, 2017, pp. 126-131, <http://dx.doi.org/10.1016/j.childyouth.2017.06.002>.

<sup>25</sup> A. GARDE, *The Best Interests of the Child and EU Consumer Law and Policy: A Major Gap between Theory and Practice?*, in J. Devenney, M. Kenny (eds.), "European Consumer Protection: Theory and Practice", Cambridge, Cambridge University Press, 2012, 164 p.

Sotto il profilo commerciale un punto centrale è costituito dalla protezione del minore rispetto all'attività di profilazione, che oggi viene indiscriminatamente e massicciamente adottata.

Sul tema specifico è stata sottoposta a pubblica consultazione la bozza delle linee guida in tema di profilazione (*Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679, wp251*) che sottolinea con disappunto come l'impatto per i minori della profilazione sia richiamato soltanto nei considerando e non nel testo del regolamento. Questa omissione appare ancora più inspiegabile se si pensa alle risultanze di uno studio pubblicato nel 2015 e commissionato dalla stessa Unione europea, in cui vengono espressamente evidenziate le criticità del marketing mirato ai bambini<sup>26</sup>.

### 3. LA TUTELA DEI MINORI NEL GDPR

#### 3.1. Età del consenso

L'indicazione è di 16 anni, lasciando però margine agli Stati membri di indicare un'età comunque non inferiore a 13 anni<sup>27</sup> con riserva di legge. Del resto, uno sguardo comparatistico agli Stati Uniti ci indica immediatamente che la soglia dei 13 anni sarebbe l'unica realmente "globale" in quanto prevista dalla locale regolamentazione (COPPA).

Sotto la soglia minima è richiesto un consenso esplicito dei genitori, o di chi esercita la responsabilità, oppure che il consenso espresso dal minore sia autorizzato dai suddetti<sup>28</sup>. Il titolare dovrà fare ogni sforzo ragionevole per verificare che il consenso sia effettivamente prestato dai genitori. Sicuramente è solo riferito all'on line, mentre off line restano validi i criteri tradizionali.

<sup>26</sup> F. LUPIÁÑEZ-VILLANUEVA, G. GASKELL, G. VELTRI et al., *Study on the impact of marketing through social media, online games and mobile applications on children's behaviour. Final Report*, March 2016.

<sup>27</sup> La mappa attuale dell'età del consenso nei diversi Stati dell'Unione non evidenzia un'età prevalente, <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751>.

<sup>28</sup> Sul consenso dei minori nel GDPR cfr. F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in "Diritto dell'informazione e dell'informatica", 2018, n. 1, p. 27; M. MACENAITE, E. KOSTA, *Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?*, in "Information & Communications Technology Law", vol. 26, 2017, n. 2, pp. 146-197; S. VAN DER HOF, *I agree... Or Do I? – A Rights-based Analysis of the Law on Children's Consent in the Digital World*, in "Wisconsin International Law Journal", vol. 34, 2017, n. 2, pp. 409-445.

Il consenso, in generale, è definito dal regolamento come «un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano»<sup>29</sup>.

Il margine di discrezionalità lasciato dalla Commissione europea ha sollevato numerose perplessità tra i commentatori<sup>30</sup>. La scelta pare motivata dall'esistenza, in alcuni ordinamenti di Stati membri, di normative che indicano età differenti, segnatamente Spagna e Olanda. In particolare ci si interroga sulle conseguenze in ordine all'effettività nel cyberspazio dei diritti riconosciuti ai fanciulli nella Convenzione internazionale sui diritti dell'infanzia (CDIA), approvata dall'Assemblea generale delle Nazioni unite il 20 novembre 1989 a New York, dal diritto al libero accesso e alla condivisione di informazioni (art. 13) alla libertà di espressione del proprio pensiero (art. 14). Inoltre, verrebbe leso anche il diritto «alla libertà di associazione e alla libertà di riunirsi pacificamente» previsto dall'art. 15 della CDIA, dal momento che tale diritto trova piena esplicazione nell'utilizzo di social network, forum e community digitali. In particolare l'art. 13 co. 1 della CDIA sancisce espressamente: «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». A meno che non si vogliano invocare i limiti previsti dallo stesso art. 13, co. 2, vale a dire il «rispetto dei diritti o della reputazione altrui» oppure la «salvaguardia della sicurezza nazionale, dell'ordine pubblico, della salute o della moralità pubbliche», ma a una prima analisi appare francamente improbabile.

Per completare il quadro degli strumenti contenuti nel GDPR direttamente incidenti sulla posizione del minore vanno menzionate le questioni legate alla trasparenza nelle informative<sup>31</sup>, al diritto all'oblio, anche quando il consenso è stato prestato da minore poi maggiorenne, e infine al ruolo dei codici di

<sup>29</sup> Più in generale sul consenso I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in "Diritto mercato tecnologico", 25 gennaio 2017.

<sup>30</sup> Tra i commenti a prima lettura si veda A. SCHIAVON, *Minori online: qual è l'età del consenso digitale?*, [cild.eu/blog/2018/01/12/minori-online-qual-e-leta-del-consenso-digitale/](http://cild.eu/blog/2018/01/12/minori-online-qual-e-leta-del-consenso-digitale/), 2018 e S. CEDROLA, *L'età del "consenso digitale" secondo il GDPR*, <http://aitra.it/leta-del-consenso-digitale-secondo-il-gdpr>, 1° febbraio 2018.

<sup>31</sup> X. CAI, W. GANTZ, *Online Privacy Issues Associated with Web Sites for Children*, in "Journal of Broadcasting and Electronic Media", vol. 44, 2000, n. 2, pp. 197-214.

condotta e regolamentazione, che all'art. 40 vengono espressamente indicati come strumenti da incentivare<sup>32</sup>.

### 3.2. *Informativa*

Riguardo al primo profilo menzionato, va ricordato come lo schema del *notice and consent* rappresenti il pilastro del modello europeo di privacy, come tale contrapposto alla filosofia statunitense dell'*opt out*. In questo senso il GDPR si propone di rendere più efficace lo strumento dell'informativa, che molto spesso si traduce in un orpello. Conformemente alle discipline in ambito di tutela dell'investitore, viene sottolineata l'importanza della trasparenza per ottenere il risultato di un consenso realmente informato. Oltre a costituire un principio generale del trattamento (art. 5, par. 1, lett. a)), l'osservanza di questo requisito è precisamente richiesto dall'art. 12 che introduce l'obbligo di garantire che le informazioni fornite agli interessati siano concise, trasparenti e redatte in un linguaggio semplice «in particolare nel caso di informazioni destinate specificamente ai minori». Ulteriormente, il considerando n. 58, rafforzando la centralità della tutela dei bambini, prevede che «quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa facilmente capire».

### 3.3. *Diritto all'oblio*

Anche il controverso “diritto all'oblio” che ha trovato spazio nel regolamento all'art. 17, significativamente rubricato *Diritto alla cancellazione («diritto all'oblio»)*, si atteggia in maniera peculiare nel caso di esercizio da parte di un minore. Come evidenziato in premessa, le ripercussioni sulla proiezione futura della vita di un individuo maggiorenne sono incrementalmente più rilevanti con riferimento agli eventi occorsi e pubblicati on line quando era ancora minorenne. Per questo motivo il diritto alla cancellazione dei dati, già presente all'art. 7, co. 3, lett. b) del Codice privacy, viene rafforzato dal GDPR con la previsione dell'obbligo per i titolari, che abbiano pubblicato dati personali oggetto di richiesta di rimozione da parte dell'interessato, di informare altri titolari che trattano quei dati con altre modalità comprese «qualsiasi link, copia o riproduzione» (art. 17, par. 2 GDPR). Il comma succes-

<sup>32</sup> D. WALSH, J.M. PARISI, K. PASSERINI, *Privacy As a Right Or As a Commodity in the Online World: The Limits of Regulatory Reform and Self-regulation*, in “Electronic Commerce Research”, 2017, n. 2.

sivo dello stesso art. 17 introduce alcune significative eccezioni all'obbligo di cancellazione, ove il trattamento risulti necessario per l'esercizio della libertà di espressione o per l'adempimento di un obbligo legale o per l'esecuzione di un compito nel pubblico interesse o nell'esercizio di pubblici poteri, o per motivi di interesse pubblico nel settore della sanità pubblica, o per fini di archiviazione nel pubblico interesse, ricerca scientifica, o storica o per fini statistici o, infine, per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. In tutti queste ipotesi, l'interesse del minore dovrà essere oggetto di opportuno bilanciamento e considerazione.

A seguito di revoca del consenso al trattamento (cfr. art. 17, par. 1 GDPR), l'interessato ha pertanto diritto alla cancellazione dei dati personali già lecitamente trattati dal titolare. Come esplicitato dal considerando n. 65, se l'interessato che richiede l'eliminazione dei dati personali ha prestato il proprio consenso quando era minore e, quindi, non era necessariamente consapevole delle conseguenze derivanti dal trattamento, questi dovrebbe poter esercitare tale diritto indipendentemente dal fatto di non essere più minore.

Una disciplina già complessa che andrà poi raccordata con le competenze del Garante privacy derivanti dalla legge italiana sul cyberbullismo.

#### *3.4. Codici di condotta, vigilanza e autoregolamentazione*

Sotto il profilo dell'autoregolamentazione, le associazioni che promuovono la tutela dei fanciulli da tempo richiedono a gran voce l'approvazione di un codice di autoregolamentazione per i fornitori di servizi di social network.

Oggi la disciplina dell'art. 40, lett. g), par. 2 GDPR prevede espressamente 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 regolamento stesso relativamente a: «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 considerando n. 77 rafforza ulteriormente il concetto che le best practice debbano confluire nei summenzionati codici di condotta ed essere incentivate proprio dalla loro adozione. Ove ci si ritrovasse con una frammentazione normativa in cui diversi Stati membri optino per diverse soglie di età al consenso del trattamento dei dati dei minori per i servizi on line, lo strumento di un codice di condotta con una forte adesione dei principali operatori potrebbe favorire una maggiore uniformità applicativa a garanzia dei minori europei.

Parimenti è fondamentale prevedere un raccordo e un coordinamento tra le attività delle autorità amministrative concorrenti. Il primo referente è rappresentato dal Garante per la protezione dei dati personali (Garante privacy), il cui ruolo verrà ulteriormente amplificato dalla costituzione del comitato europeo per la protezione dei dati competente a valutare l'attuazione del GDPR. Ai sensi della normativa da ultimo richiamata, le autorità di controllo nazionale devono (art. 57(1)(b)) tenere in debito conto la tutela dei minori. Sotto questo profilo si può qui richiamare l'attività informativa con un opuscolo del garante italiano pubblicato nel 2009<sup>33</sup>, che si colloca nel solco dell'impegno del garante europeo<sup>34</sup>.

Sul tema specifico è stata costituita nel 2011 l'Autorità garante per l'infanzia e per l'adolescenza<sup>35</sup>. Inoltre l'Autorità per le garanzie nelle comunicazioni (AGCOM) con la delibera n. 481/14/CONS ha istituito l'*Osservatorio delle garanzie per i minori e dei diritti fondamentali della persona su Internet* introducendo tra i suoi compiti l'analisi del fenomeno dei social network e la verifica delle policy adottate dai principali operatori del settore. Per quanto questa iniziativa sia stata discussa, è da ricordare che la legge istitutiva prevede fra i compiti istituzionali dell'Autorità quello della tutela dei minori.

Va ricordato in ogni caso come la disciplina che regola il commercio elettronico e taluni servizi della società dell'informazione (art. 5 co. 1 lett. a), d.lgs. 70/2003), espressamente attribuisce all'autorità amministrativa competente il potere di limitare i servizi della società dell'informazione provenienti da altro Stato membro, anche per "la tutela dei minori".

<sup>33</sup> Analogamente, vedi l'omologa francese CNIL - COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Editeurs de sites pour enfants: n'oubliez pas vos obligations!*, 2 settembre 2015, <https://www.cnil.fr/fr/editeurs-de-sites-pour-enfants-noubliez-pas-vos-obligations-0>.

<sup>34</sup> G. BUTTARELLI, *The Children Faced with the Information Society*, relazione presentata dal Garante europeo per la privacy al 1<sup>st</sup> Euro-Ibero American Data Protection Seminar on "Children's Protection" (Cartagena de Indias, 26 May 2009). Vedi inoltre EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), *Opinion on the Communication "A Comprehensive Approach on Personal Data Protection in the European Union"*, [https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14\\_Personal\\_Data\\_Protection\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf), 2011, in cui espressamente il Garante europeo sottolinea l'esigenza di specifiche disposizioni nel GDPR per proteggere gli interessi dei bambini e garantire la certezza del diritto per i titolari del trattamento.

<sup>35</sup> L'Autorità è stata istituita con l. 12 luglio 2011, n. 112.

In un quadro che resta fluido in attesa di conoscere l'opzione del legislatore italiano<sup>36</sup> e, più in generale, dei diversi Stati membri dell'Unione europea riguardo all'età minima per poter esprimere un valido consenso al trattamento dei dati personali on line, risulta prematuro esprimere conclusioni definitive sull'impatto del nuovo regolamento privacy con riguardo alla tutela del minore. L'occasione del GDPR è senz'altro quella di ripensare la tutela del minore on line; si richiedono regole globalmente riconosciute e caratterizzate da una certa uniformità, per favorire la compliance da parte dei provider di servizi, le cui associazioni di categoria potranno svolgere un ruolo propulsore in coordinamento con le autorità garanti.

Considerato però il complessivo scenario in cui i dati personali sono raccolti in maniera sempre più massiccia e sono oggetto di mercificazione in cambio di vantaggi non sempre trasparenti, il livello di guardia va mantenuto particolarmente alto per i dati dei minori, specie per la progressiva e costante interconnessione, che sarà sempre più esasperata con la diffusione delle tecnologie IoT e l'avvento delle smart city. Una recente ricerca<sup>37</sup> fotografa uno scenario desolante in cui i minori sono sempre più connessi e sempre meno preoccupati della propria privacy on line, mostrandosi inclini a rinunciare con naturalezza ai propri diritti sull'immagine e sui dati personali, come ad esempio i propri contatti, in cambio della fornitura di servizi a titolo gratuito.

La *commodification* dei dati personali, spesso trattati come un bene di scambio, rappresenta in questo caso non soltanto un "male minore" dell'economia dell'informazione, bensì in numerosi casi il male *del* minore.

<sup>36</sup> L'art. 13, l. 25 ottobre 2017, n. 163, *Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea* introduce una delega specifica per l'adeguamento della normativa nazionale al GDPR.

<sup>37</sup> Per i risultati della ricerca, condotta dall'istituto Ipsos, <https://www.savethechildren.it>, 7 febbraio 2017.