

App, Privacy e minori. La tutela dei minori in internet tra autodeterminazione informativa e fruizione dei contenuti digitali

di Pierpaolo ARGANELLI*

SOMMARIO: **1.** Introduzione. **2.** Nozione di minore in Internet. Normativa internazionale, Statunitense ed Italiana. **3.** Analisi e confronto delle social media *policies* in USA ed in Italia. **4.** Le App e il consenso prestato dal minore. **5.** Normativa e dottrina del comportamento dei minori sui social. **6.** Il complesso bilanciamento tra *policies* private e diritti fondamentali. **7.** Il ruolo dello Stato italiano e dell'Europa nella protezione dei dati dei minori. **8.** Prospettive regolatorie per le sfide in atto e che verranno.

ABSTRACT: *The article will analyse the relationship between social networks world and minors. Starting from a comparative analysis between definitions of minor under International law, US and Italian legal systems, the article will show the complexity of balance between persons' fundamental rights. It will focus on minor as sensitive individual who needs to be protected more than how it is currently. The analysis of European privacy law under the new GDPR and of Italian constitutional principles like self-determination of individuals and of social networks policies will try to show the current situation and what are the future perspectives.*

1. Introduzione.

I minori sono sempre più immersi nelle nuove tecnologie e negli strumenti di comunicazione ed informazione, comprendendone immediatamente l'utilizzo, ma non avendo sempre una sufficiente consapevolezza dei rischi e dei possibili effetti negativi che possono scaturire da un uso non attento ed incontrollato di questi strumenti¹. Al tempo stesso i *social media* e le *chat*

* Dottorando di ricerca in "Diritto dei servizi nell'ordinamento italiano ed europeo", Università degli Studi di Napoli Parthenope e Data Protection Officer.

¹ Sui rischi dovuti all'uso dei dati e della connettività in maniera impropria si ricorda: D. LUPTON e B. WILLIAMSON, *The Datafied Child: The Dataveillance of Children and Implications for Their*

stanno svolgendo un ruolo determinante nel vissuto di minori in formazione sia da un punto di vista educativo che personale. In particolare, i *social* rappresentano sovente il principale accesso all'informazione da parte dei minorenni, il che si traduce in una costante esposizione degli stessi alle più svariate pubblicità, a *fake news*, a comunicazioni, politiche e non, che inevitabilmente finiscono per influenzare la loro visione del mondo e la loro personalità².

Può considerarsi opinione condivisa che, nel mondo dei *social*, spesso i minori sono autori o vittime di comportamenti che nel mondo reale non sarebbero possibili³ e che la creazione di nuovi e più coinvolgenti *social network* e la presenza di poche⁴ grandi compagnie *high-tech*, spesso straniere, pongano a rischio la tutela dei dati dei minori ed il loro diritto ad autodeterminarsi⁵.

Rights, in *New Media & Society*, vol. 19, 2017, n. 5, pp. 780-794. Se si vuole approfondire il tema focalizzandosi sull'impatto nel lungo periodo di uno uso non attento dei social nella vita del minore si suggerisce un recente studio di G. BERMAN. e K. ALBRIGHT, *Children and the Data Cycle: Rights and Ethics in a Big Data World*, INNOCENTI Working Paper 2017, 5, Firenze, UNICEF Office of Research, 2017.

² Per un *excursus* storico si rimanda a J. VAN DIJCK, *The Culture of Connectivity: A Critical History of Social Media*, Oxford, Oxford University Press, 2013. Da osservare anche come l'attenzione è l'obiettivo dei gestori dei servizi on line vedi l'analisi di T. WU, *The Attention Merchants: The epic scramble to get inside our Heads*, New York, ALFRED A. KNOPF, 2016 e l'introduzione dell'articolo di G. PEDRAZZI: *Minori e social media: tutela dei dati personali, autoregolamentazione e privacy*, Informatica e diritto, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 437-451.

³ Pensiamo ai c.d. "leoni da tastiera" ribattezzati anche come "*haters*". Gente che sui social media sfoga la propria rabbia repressa accumulata nel quotidiano comportandosi sui social media in modi spesso passibili di denuncia. Fra i molti si possono ricordare gli insulti a sfondo razziale rivolti alla senatrice Segre su Twitter, Facebook ecc., gli insulti a sfondo sessuale e non solo alle donne che avevano denunciato casi di stupro.

⁴ Vedi acquisizione da parte di Facebook prima di Instagram e poi di WhatsApp per miliardi di dollari fra i molti: per Instagram nel 2012: <https://st.ilsole24ore.com/art/tecnologie/2012-04-09/facebook-acquista-instagram-miliardo-193539.shtml?uid=AbUbtaLF>, per WhatsApp nel 2014: <https://st.ilsole24ore.com/art/notizie/2014-02-19/facebook-compra-whatsapp-19-miliardi-dollari-231641.shtml?uid=AB3q4lx>.

⁵ A tal fine si osservi il report *Norwegian Consumer Council, #WatchOut Analysis of Smartwatches for Children*, <https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf>, 2017.

Il presente lavoro si svilupperà a partire dal concetto di minore nell'ordinamento italiano e statunitense⁶. Saranno analizzate le prospettive regolatorie nazionali ed europee in merito all'accesso, ai comportamenti ed in generale all'interazione con i social networks da parte del minore. Ci si soffermerà inoltre sulle policies⁷ adottate per assicurare una maggiore protezione dei propri utenti che, tra gli altri, hanno anche l'obiettivo di "proteggere" in modo particolare i minori⁸.

2. Nozione di minore in Internet. Normativa internazionale, Statunitense ed Italiana.

A livello internazionale una prima definizione di minori si trova nella Convenzione ONU sui diritti dell'infanzia e dell'adolescenza⁹, la quale definisce il minore, art.1, come: "ogni essere umano avente un'età inferiore a

⁶ Si è deciso di scegliere gli USA in quanto le maggiori compagnie *high-tech* hanno la loro sede principale lì e di conseguenza le *policies* che disciplinano l'utilizzo dei loro software e delle loro app sono di estrazione giuridica nord-americana.

⁷ Nel corso di questo articolo saranno analizzate, infatti, le *policies* delle compagnie social appena citate e si vedrà come moltissimi minori e genitori non rispettino queste policies ed anzi le aggirino per i motivi più vari: convenzioni sociali, comodità, ignoranza ecc. Queste *policies*, in alcuni casi, cambiano da Paese a Paese. Questo aspetto sarà analizzato concentrandosi sulle diversità degli ordinamenti USA e Italia. Un confronto questo che mira a sottolineare come l'età dei ragazzi scelta dal paese determinerà poi lo sviluppo delle nuove generazioni. In relazione all'adozione di idonei ed effettivi strumenti di tutela, è importante anche identificare la percezione dei minori stessi rispetto ai rischi connessi all'utilizzo di social media cercando di capire se la volontà del legislatore nazionale di riformare il diritto di voto⁷, il diritto di guida *et alter* diminuendo l'età dai 18 ai 16 anni può coincidere con la necessità di maggior tutela in rete.

⁸ Questo a causa del *privacy paradox*. Il quale nella letteratura sociologica viene definito come "la tendenza per i soggetti 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" vedi fra i molti: 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, "Rassegna di diritto civile", 2016, n. 4, p. 1324 ss. Si pensi ad esempio al limite di età per l'iscrizione ad un social e la necessaria autorizzazione dei genitori che rappresenta un aspetto critico con riferimento alla difficoltà di verificare la veridicità dell'autorizzazione.

⁹ Convention on the Rights of the Child - CRC, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989, e ratificata dall'Italia il 27 maggio 1991 con la legge n. 176.

diciott'anni, salvo se abbia raggiunto prima la maturità in virtù della legislazione applicabile”¹⁰.

Nella medesima Convenzione si rinviene anche la fissazione del principio del “superiore interesse”, sancito dall’art. 3, in base al quale “in ogni legge, provvedimento, iniziativa pubblica o privata e in ogni situazione problematica, l’interesse del bambino/adolescente deve avere la priorità” e dall’art.16¹¹ che sancisce il diritto di ogni minore a non subire interferenze arbitrarie o illegali con riferimento alla vita privata, alla sua corrispondenza o al suo domicilio; è altresì riconosciuto il diritto del minore a non subire lesioni alla sua reputazione e al suo onore.

Strettamente collegato all’art.16 è poi l’art.17¹² il quale prevede il dovere da parte di ogni Stato di riconoscere l’importanza della funzione esercitata dai *mass-media*, in quanto mezzi idonei a garantire ma anche a ledere una sana crescita e una corretta formazione del minore stesso¹³. In quest’ultimo caso

¹⁰ Tale Convenzione è stata ratificata da 196 Stati e rappresenta un testo giuridico di eccezionale importanza poiché riconosce, in forma coerente, tutti i minori del mondo come titolari di diritti civili, sociali, politici, culturali ed economici. È composta di 54 articoli e da tre Protocolli opzionali, concernenti i bambini in guerra, lo sfruttamento sessuale e le procedure di reclamo. La parte che più interessa ai fini di questo lavoro è la prima che enuncia i diritti di cui i minori sono titolari (artt.1-41).

¹¹ Si veda articolo 16: «1. *No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.* 2. *The child has the right to the protection of the law against such interference or attacks*». Per ulteriore approfondimento in merito al contenuto della Convenzione si consulti: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>.

¹² Si veda Articolo 17: «*States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health. To this end, States Parties shall: (a) Encourage the mass media to disseminate information and material of social and cultural benefit to the child and in accordance with the spirit of article 29; (b) Encourage international co-operation in the production, exchange and dissemination of such information and material from a diversity of cultural, national and international sources; (c) Encourage the production and dissemination of children’s books; (d) Encourage the mass media to have particular regard to the linguistic needs of the child who belongs to a minority group or who is indigenous; (e) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18*». Per ulteriore approfondimento in merito al contenuto della Convenzione si consulti: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx>.

¹³ Gli Stati parti riconoscono l’importanza della funzione esercitata dai mass media e vigilano affinché il fanciullo possa accedere a una informazione e a materiali provenienti da fonti

si parla anche di libertà del minore di autodeterminarsi, diritto fondamentale riconosciuto anche all'art.2 della nostra Costituzione¹⁴.

In USA ed in Italia sono definiti come "minori" tutti coloro che hanno meno di 18 anni¹⁵. In Italia, al compimento dei 18 anni il minore acquista la piena capacità di intendere e di volere e quindi di autodeterminarsi, diventando responsabile civilmente di tutte le sue scelte ed imputabile penalmente per le scelte sbagliate che potrebbe compiere. Il che per definizione negativa significa che prima dei 18 anni egli/ella è in formazione come persona.

Dal punto di vista civilistico, i genitori esercenti la potestà sono responsabili dei reati e degli illeciti commessi sia dal minore fra i 14 ed i 17 anni nei confronti di chiunque, minore e non, sia del minore fino ai 14 anni di età vista l'incapacità totale e la non imputabilità¹⁶.

Tuttavia, dal punto di vista penalistico, in merito alla nozione di minore nel panorama italiano, è necessario ricordare la differenza tra gli infra-diciottenni e gli infra-quattordicenni. Infatti, secondo il codice penale: "il minore di 14 anni che commette un reato non è punibile in quanto totalmente incapace di intendere e di volere" mentre "è imputabile chi, nel momento in cui ha commesso il fatto, aveva compiuto 14 anni ma non ancora i 18, se aveva capacità di intendere e di volere"¹⁷. Di conseguenza, parlando di capacità di

nazionali e internazionali varie, soprattutto se finalizzati a promuovere il suo benessere sociale, spirituale e morale nonché la sua salute fisica e mentale. A tal fine, gli Stati parti: incoraggiano i mass media a divulgare informazioni e materiali che hanno una utilità sociale e culturale per il fanciullo e corrispondono allo spirito dell'art. 29; incoraggiano la cooperazione internazionale in vista di produrre, di scambiare e di divulgare informazioni e materiali di questo tipo provenienti da varie fonti culturali, nazionali e internazionali; incoraggiano la produzione e la diffusione di libri per l'infanzia; incoraggiano i mass media a tenere conto in particolar modo delle esigenze linguistiche dei fanciulli autoctoni o appartenenti a un gruppo minoritario; favoriscono l'elaborazione di principi direttivi appropriati destinati a proteggere il fanciullo dalle informazioni e dai materiali che nuocciono al suo benessere in considerazione delle disposizioni degli artt. 13 e 18.

¹⁴ Si veda sul punto autorevole dottrina: A.PAPA, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Giappichelli, 2009

¹⁵ Si veda art. 97 e 98 c.p. il primo indica che il minore sotto i quattordici anni non è mai imputabile, il secondo che "è imputabile chi, nel momento in cui ha commesso il fatto, aveva compiuto 14 anni ma non ancora i 18, se aveva capacità di intendere e di volere".

¹⁶ Questo spesso al contrario di molti degli Stati in cui le compagnie social sono nate e dove hanno il loro quartier generale.

¹⁷ La dottrina e la giurisprudenza sono talmente numerose e univoche sul concetto di imputabilità che si può affermare che: per poter procedere penalmente nei confronti di un

intendere e di volere un minore con un'età tra i 14 ed i 17 anni si può dire abbia una "capacità parziale"¹⁸ in quanto essa deve essere accertata e non è presunta come per gli adulti.

Negli Stati Uniti d'America, la nozione di minore e la regolamentazione delle relazioni familiari è affidata ad ogni stato federale¹⁹. La legge federale USA fornisce solo il "cappello" entro cui gli stati federali devono disciplinare le singole fattispecie appartenenti al diritto di famiglia. La legge federale americana e la sua interpretazione giurisprudenziale fornisce la seguente definizione:

«a person who does not have the legal rights of an adult. A minor is usually defined as someone who has not yet reached the age of majority. In most states, a person reaches majority and acquires all of the rights and responsibilities of an adult when he or she turns 18»²⁰.

Questa definizione è volutamente vaga in quanto ogni stato della federazione disciplina autonomamente i requisiti per accedere alla maggiore età²¹. La legge federale americana prima citata stabilisce inoltre che:

«Until a minor reaches the legal age of adulthood, he or she may not be responsible for his/her own actions (including the capacity to enter into a contract which is enforceable by the other party), for damages for

minore è necessario che questi sia imputabile, ovvero che sia stata valutata la capacità del minore per essere dichiarato responsabile di un reato ed essere sottoposto a una pena. In base a quanto detto nella nota precedente: ai sensi dell'art. 98 del c.p., per i minori dai 14 ai 17 anni la capacità di intendere e di volere in relazione al reato compiuto deve essere sempre accertata, mentre per gli adulti autori di reato è presunta

¹⁸ Fra i molti, in ordine cronologico la più recente decisione che afferma una "capacità parziale" è stata espressa dalla Corte di Cassazione penale con la sentenza n. 10478 del 2 marzo 2017.

¹⁹ Per un excursus storico si consiglia: J.V.CALVI e S.COLEMAN, *American Law and legal system*, 2005, Pearson Education, pag.305-326

²⁰ *Dictionary of Legal Terms: A-D*. (2011), in D. BATTEN, *Gale Encyclopedia of American Law, 3rd edition*, Vol. 14, Detroit, MI, USA, p. 14; 18 U.S.C. § 2256- *Definitions*, consultabile al link: <https://www.law.cornell.edu/uscode/text>; U.S. Legal, *Age of Majority Law and Legal Definition* consultabile al link: <https://definitions.uslegal.com/a/age-of-majority/>.

²¹ Per un approfondimento analitico si suggerisce di visitare il seguente link: https://www.law.cornell.edu/wex/table_emancipation dal quale si evince come: la maggior'età si raggiunge a 18 anni in 49 Stati, ad eccezione del Mississippi dove essa si acquisisce a 21 anni, dell'Alabama e del Nebraska dove si acquisisce a 19.

negligence or intentional wrongs without a parent being liable, nor for punishment as an adult for a crime»²².

In tutte le situazioni appena descritte i responsabili saranno quindi i genitori²³, i quali potranno incorrere in conseguenze sia penali, rimanendo ovviamente una responsabilità in capo al minore per i reati commessi, che civili. In alcuni casi, infatti, lo Stato avrà anche il diritto di togliere il minore dalla custodia²⁴ genitoriale. La *ratio* di questa procedura è tutelare l'interesse del minore e l'interesse pubblico alla sua educazione²⁵.

L'unica eccezione alla regola generale appena riportata è rappresentata dalla commissione di un crimine particolarmente grave commesso dal minore come ad esempio l'omicidio, lo stupro o la rapina a mano armata per i quali è possibile processare il minore avente almeno 13 anni come un adulto²⁶ e lo stesso minore sarà eventualmente condannabile alla pena capitale se di età maggiore di 16 anni²⁷. È importante anche porre l'attenzione su ciò che concerne altri diritti del minore come: «*the marriage with or without parental consent, driving, prosecution for crimes, the right to choose an abortion and liability for damages*» anche se queste variano da Stato a Stato²⁸. I genitori

²² Vedi nota n.16

²³ Per un approfondimento sulla responsabilità genitoriale ed i suoi limiti negli Stati Uniti si legga ad esempio il seguente passo tratto da autorevole dottrina: "The primary parental responsibilities toward children are twofold: 1. To provide the basic necessities of food, shelter, and clothing and 2. To provide care, control, supervision, education, and reasonable discipline" J.V. CALVI e S. COLEMAN, *American Law and legal system*, 2005, Pearson Education, pag.324. La "reasonable education" è stata ed è ancora oggetto di dibattito nella dottrina americana in quanto viene a volte distortamente usata per difendere gli accusati di abuso minorile e maltrattamenti. Il senso di tale dettame federale è da ricercarsi piuttosto nel fatto che uno scappellotto se necessario è consentito, altre pratiche come picchiarlo pesantemente, rompergli un arto, ustionarlo ecc. no. Altri casi al riguardo: Hunt vs Thompson approfondito da S.P. BRECKINRIDGE, *the Family and the State*, University of Chicgo Press, 1934, p.242.

²⁴ Vedi PRINCE v. MASSACHUSSETS, 321 U.S. 158 (1944), pag.171: "the family itself is not beyond regulation in the public interest".

²⁵ Vedi il caso scolastico: WISCONSIN vs YODER, 406 U.S.205 (1972). L'agenzia dei servizi sociali potrà infatti ottenerne la custodia temporaneamente (se i genitori si dimostreranno collaborativi) o permanentemente (fino al compimento della maggiore età).

²⁶ Vedi *Congressional Quarterly* 52, 11 (19 Marzo 1994): 672 e 52,34 (27 Agosto 1994): 2490.

²⁷ Vedi Thompson vs Oklahoma, 487 U.S. 815 (1988)

²⁸ Ad esempio, per quanto concerne il matrimonio, il requisito dell'età minima è basato su una serie di fattori presi in considerazione in maniera diversa da ogni singolo stato federale. Questi fattori sono: biologici cioè legati a quando viene stabilita l'età della pubertà; tradizionali, legati

o gli esercenti responsabilità genitoriale americani hanno il "*duty of care, support and supervision*"²⁹ del minore. Un'altra particolarità nell'ambito del diritto civile americano è che "*a contract, otherwise valid, entered into by a minor, cannot be disaffirmed because of the minor's minority if the contract is to pay the reasonable value of necessities*"³⁰.

3. Analisi e confronto delle social media *policies* in USA ed in Italia.

Com'è noto, ogni azienda ha le sue *policies* e strategie di mercato che mirano ad attrarre il maggior numero di consumatori³¹, a rinforzare l'immagine del brand ed in generale come fine ultimo a massimizzare i profitti magari sfruttando economie di scala e vantaggi comparati rispetto ad altri competitors. Tutto ciò è valido anche per le aziende che si occupano di *social networking*³².

Queste *policies* debbono necessariamente tener conto dei principi giuridici generali e delle leggi dei singoli Stati nei quali operano le norme in materia di tutela del pensiero ne rappresenta un esempio il minore.

quindi alle tradizioni culturali di ogni singolo stato utili per stabilire l'età minima per contrarre matrimonio; e legali cioè legati alle differenti *contract laws* previste.

²⁹ J.V. CALVI e S. COLEMAN, *American Law and legal system*, 2005, Pearson Education, pag.321

³⁰ Inoltre: «*The meaning of the term "necessaries" depends on the facts of the individual case. It depends on many things, including the particular circumstances of the minor, the actual need, and the use to which the purchased article is to be put. However, the common-law classification of necessities as including food, lodging, clothing, medicine, medical attention, and education is generally recognized to the extent such items are suited to the minor's social position and situation in life, even though such items are not absolutely needed*».

³¹ Il loro obiettivo generale e primario è quello di aumentare il numero di consumatori. Il motivo è semplice grazie all'iscrizione e all'utilizzo dell'utente la piattaforma social acquisisce informazioni dell'iscritto e grazie al consenso più o meno cosciente, vende le informazioni acquisite ad altre aziende; le quali grazie a tali informazioni possono meglio profilare il loro possibile cliente e quindi adottare strategie di marketing e di sfruttamento degli spazi pubblicitari del social in maniera più efficiente ed efficace. Ovviamente, tutto questo premesso, rientra nella libertà di iniziativa economica privata disciplinata in Italia dall'art.41 Cost., che garantisce l'autonomia di ciascun imprenditore nel dirigere la propria impresa. Appare pacifico affermare che il diritto e le sue declinazioni cambino da Stato a Stato e che quindi questo adattamento delle *policies* ne sia naturale conseguenza.

³² È bene sottolineare come alcune grandi aziende high-tech che operano prevalentemente nel mondo social, ad esempio Facebook, abbiano diverse *policies* di iscrizione, e quindi di accesso al servizio da loro offerto, a seconda dello Stato o del Continente in cui operano la raccolta dei dati.

La Facebook Inc. ha acquisito Instagram nel 2012 e WhatsApp nel 2014 ed ha, tuttavia, applicato tre *polices* diverse³³. Nella propria *policy*, Facebook richiede all'utente di essere responsabile nella creazione del suo account senza però avere nessun metodo di verifica delle informazioni fornite dallo stesso e senza prevedere serie conseguenze in caso di violazione della *policy*. Queste lacune hanno permesso nel tempo la nascita di migliaia di profili falsi, doppi, tripli infrangendo le prime due richieste della *policy*. Inoltre, bisogna sottolineare come Facebook imponga un'età minima di 13 anni per iscriversi. In Instagram l'età minima per iscriversi è la stessa, al contrario per quanto riguarda WhatsApp l'età minima per iscriversi è 16 anni. Questa differenza fa sorgere alcuni interrogativi. Infatti, Facebook Inc, ponendo l'età minima a 13 anni, fa sì che anche utenti del tutto privi di capacità di intendere e di volere (quella parziale come detto si acquisisce a 14 anni ed è comunque sempre da dimostrare) possano sottoscrivere quello che nei fatti è un contratto di servizio che, come forma di pagamento, ha il consenso al trattamento dei propri dati³⁴.

³³ In Italia consultando la policy di Facebook si legge al punto 1 della stessa: "Chi può usare Facebook: [...] l'utente è tenuto a: 1. usare lo stesso nome di cui si serve nella vita reale; fornire informazioni personali accurate; 2. creare un solo account (il proprio) e usare il proprio diario per scopi personali; 3. non condividere la propria password, non concedere l'accesso al proprio account Facebook ad altri o trasferire il proprio account ad altri (senza l'autorizzazione di Facebook). L'obiettivo è rendere Facebook disponibile a tutti, ma il suo uso è proibito a: utenti che hanno meno di 13 anni." La scelta di quest'età alla luce di quanto sopra riportato in termini di diritto penale americano ci deve far riflettere. Inoltre, la policy continua: "utenti condannati per violenza sessuale; utenti con account disabilitati in precedenza per violazione delle Condizioni o Normative di Facebook; utenti non autorizzati dalla legge applicabile a ricevere prodotti, servizi o software di Facebook". Consultabile al link: <https://it-it.facebook.com/legal/terms>

³⁴ Il che secondo quanto riportato dal Garante della Privacy e dal diritto italiano è lesivo della sua privacy. Infatti, è noto che, in teoria, l'Italia abbia fissato a 14 l'età minima per poter prestare validamente consenso ai servizi della società dell'informazione, Il comma 1 dell'art. 2-quinquies del novellato Codice Privacy ed introdotto dal D.Lgs. 101/2018 dispone: "In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale". Il perché Facebook Inc. non abbia modificato tale policy che fissa invece età minima a 13 anni quindi rimane un mistero.

Inoltre, accetta di esporre un ragazzo tredicenne ad una serie di pubblicità e di informazioni, spesso non controllate, che sicuramente avranno un impatto sulla sua crescita ed autodeterminazione, e ledendo il diritto all'autodeterminazione dell'individuo³⁵ sancito dall'art.2 della Costituzione e dagli articoli 16 e 17 della Convenzione ONU sopra citati. Facebook INC con questa *policy* accetta anche il rischio che l'infra-quattordicenne possa porre in essere comportamenti lesivi per sé stesso e per gli altri³⁶.

Un'altra questione su cui è importante riflettere è che sebbene un minore sia sotto la responsabilità dei genitori, gli stessi per ammissione e previsione delle social policies non possono in alcun modo avere accesso all'account del figlio/a senza il suo consenso³⁷. L'unico modo per ottemperare a quanto previsto dal GDPR³⁸ e successiva legge di recepimento è che il genitore o i genitori si iscrivano al social e prestino il loro consenso alla nascita del social

³⁵ Sull'interazione uomo-macchina e sui riflessi che questa ha sui diritti all'autodeterminazione e all'identità personale dell'individuo la dottrina si sta interrogando da tempo. Il tema sarà poi ripreso nei paragrafi successivi. Tuttavia, senza avere velleità di completezza si vedano: L. AVITABILE, *Il Diritto Davanti All' algoritmo*, in *Rivista Italiana Per Le Scienze Giuridiche*, 8, 2017, Pp. 315-327; L. CALIFANO, *Brevi Riflessioni Su Privacy e Costituzionalismo al tempo dei Big Data*, in *federalismi.it*, 9, 2017, Pp. 1-7; G. D'ACQUISTO –M. NALDI, *Big Data e Privacy by Design*, Torino, 2017; F. PIZZETTI, *Intelligenza Artificiale, Protezione dei Dati Personali e Regolazione*, Torino, 2017; F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali*, Torino, 2016; G. FINOCCHIARO, *Riflessioni su Diritto e Tecnica*, in *Diritto Dell'informazione e Dell'informatica*, 4-5, 2012, P. 831 Ss.; G. RESTA, *Diritti della Personalità: problemi e prospettive*, in *Diritto dell'informazione e Dell'informatica*, 6, 2007, Pp. 1043-1071; G. RESTA, *Identità Personale e Identità Digitale*, in *Diritto dell'informazione e dell'informatica*, 3, 2007, Pp. 511-531; V.ZENO-ZENCOVICH, *Informatica ed Evoluzione Del Diritto*, in *Diritto Dell'informazione E Dell'informatica*, 1, 2003, P. 89 ss; P.BENANTI, *Digital Age. Teoria del cambio d'epoca. Persona, famiglia e società*; Edizioni San Paolo, 2020.

³⁶ Si pensi ad esempio alla *datification* ed al *cyber-bullismo* entrambi fenomeni che saranno poi trattati nei paragrafi successivi.

³⁷ La policy recita come di seguito: "Posso accedere all'account Instagram di mio figlio adolescente? Comprendiamo le tue preoccupazioni sull'uso della nostra applicazione da parte di tuo figlio, ma purtroppo non possiamo fornirti l'accesso al suo account né intraprendere alcuna azione sull'account in seguito alle tue richieste. In generale, le leggi sulla privacy non ci consentono di fornire l'accesso non autorizzato a un account a una persona diversa dal titolare. Tieni presente che tutti gli utenti di età superiore ai 13 anni sono autorizzati ad avere un account e rientrano nell'ambito di questa normativa." Vedi nei link sottostanti: <https://www.instagram.com/about/legal/terms/api/> e [https://help.instagram.com/154475974694511/?helpref=hc_fnav&bc\[0\]=Centro%20assistenza%20di%20Instagram&bc\[1\]=Centro%20per%20la%20privacy%20e%20la%20sicurezza](https://help.instagram.com/154475974694511/?helpref=hc_fnav&bc[0]=Centro%20assistenza%20di%20Instagram&bc[1]=Centro%20per%20la%20privacy%20e%20la%20sicurezza)

³⁸ Regolamento Generale sulla Protezione dei Dati n.679/2016 UE

del minore³⁹. Una ricerca del Monitor Minor del 2017 ha mostrato come sulle piattaforme social britanniche ed americane il 38% degli utenti siano bambini infra-quattordicenni con profili falsi⁴⁰. Questo dimostra come ipoteticamente i minori possano accedere ai social senza alcun controllo dei genitori o degli esercenti la responsabilità genitoriale che tuttavia rimangono gli unici responsabili delle azioni dei propri figli.

4. Le App e il consenso prestato dal minore.

Tra gli strumenti preferiti dai minori per esprimere le loro idee, studiare, giocare ed in generale autodeterminarsi ci sono le App⁴¹.

³⁹ Tuttavia, creare un profilo mentendo sull'età non è complesso e questo spesso è l'espedito più usato dai minori che vogliono tutelare la loro privacy dai genitori senza rendersi che tale tutela la stanno cedendo a terzi sconosciuti e senza tener conto dei rischi che comporta tale iscrizione.

⁴⁰ Si rimanda al rapporto presente su: <https://www.monitorminor.com>

⁴¹ Per App in generale si intende un software progettato prevalentemente per dispositivi mobili con funzioni limitate rispetto ad un software principale ma che consente all'utente in possesso del dispositivo mobile di collegarsi ad un server principale esterno o di essere egli stesso il server. Per una completa e dettagliata definizione e classificazioni delle App si cita: «*A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited function. [...] A mobile application also may be known as an app, web app, online app, iPhone app or smartphone app. Mobile applications are a move away from the integrated software systems generally found on PCs. [...] The simplest mobile apps take PC-based applications and port them to a mobile device. As mobile apps become more robust, this technique is somewhat lacking. A more sophisticated approach involves developing specifically for the mobile environment, taking advantage of both its limitations and advantages. [...] Apps are divided into two broad categories: native apps and web apps. Native apps are built for a specific mobile operating system, usually iOS or Android. Native apps enjoy better performance and a more finely-tuned user interface (UI), and usually need to pass a much stricter development and quality assurance process before they are released. Web apps are used in HTML5 or CSS and require minimum device memory since they're run through a browser. The user is redirected on a specific web page, and all information is saved on a server-based database. Web apps require a stable connection to be use. There are several types of apps currently available. Gaming apps: The equivalent of computer video games, they are among the most popular types of apps. [...] Productivity apps: These focus on improving business efficiency by easing various tasks such as sending emails, tracking work progress, booking hotels, and much more. Lifestyle and entertainment apps: Increasingly popular, these encompass many aspects of personal lifestyle and socialization such as dating, communicating on social media, as well as sharing (and watching) videos. [...] Other app types include mobile commerce (M-commerce) apps used to purchase*

Ogni App ha una propria *policy* di autoregolamentazione che in Europa trova oggi la propria interfaccia regolatoria nel Regolamento Europeo n.679 del 2016 (d'ora in poi GDPR). In particolare, l'art.40 lett.g del GDPR ha previsto espressamente la nascita di codici di condotta frutto dell'autoregolamentazione del settore in esame. Molti *social*, per avvicinarsi ai potenziali clienti minori, e non, hanno creato App scaricabili sugli *smartphone* spesso gratuitamente.

Le App presenti sul mercato necessitano del consenso digitale al trattamento dei propri dati personali come requisito necessario al funzionamento. Ove, infatti, l'utente decidesse di non prestare il consenso, accettando la *policy in toto*, non potrebbe usare l'App sul suo dispositivo.

Al fine di poter meglio comprendere il consenso nel mondo digitale è bene partire da quanto previsto dall'art. 6, par. 1, lett. a) del GDPR⁴² da leggere

goods online [...], travel apps that help a traveler in many ways (booking tours and tickets, finding their way through maps and geolocation, travel diaries, etc.), and utility apps such as health apps and barcode scanners». Si veda il link: <https://www.techopedia.com/definition/2953/mobile-application-mobile-app>.

⁴² Reg.UE n.679/2016 prevede che i trattamenti di dati basati sul consenso vengano disciplinati il quale recita: "l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità".

necessariamente in combinato disposto con i Considerandi n. 32⁴³, 42⁴⁴, 43⁴⁵ e 171⁴⁶ del medesimo regolamento⁴⁷ che stabilisce cosa s'intende per

⁴³ Il considerando recita: «Il consenso dovrebbe essere espresso mediante 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, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso». Il consenso deve essere espresso mediante un atto positivo ed inequivocabile per essere legittimo.

⁴⁴ Il quale recita: «Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio». Quindi il secondo requisito del consenso prestato è che esso deve essere consapevole.

⁴⁵ Il quale recita: «Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione». Il terzo requisito del consenso per essere valido è che esso sia espresso liberamente senza costrizioni.

⁴⁶ Questo Considerando prevede che: «Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. [...]. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del

consenso, le sue modalità di rilascio e le sue caratteristiche principali. Brevemente, possono sottolinearsi due aspetti: in primo luogo che il consenso debba essere liberamente prestato da un soggetto consapevole in modo positivo ed inequivocabile, in secondo luogo che il titolare del trattamento debba adoperarsi per accertare la validità di questo consenso tramite l'uso delle tecnologie disponibili.

Quanto appena ricordato è oggetto di una tutela rafforzata per quanto riguarda i minori. Infatti, l'art.8⁴⁸ del GDPR stabilisce al riguardo due soglie d'età.

La prima riguarda l'età minima, non derogabile, per utilizzare un social o un'app, fissata a 13 anni. A tale età il minore avrà bisogno del consenso dell'esercente la responsabilità genitoriale per acconsentire al trattamento dei dati personali.

La seconda soglia d'età che viene fissata a 16 anni invece si riferisce alla prestazione di un valido consenso autonomo. Tuttavia, quest'ultima è una soglia derogabile in base alla normativa dei singoli stati membri⁴⁹.

È importante analizzare quanto previsto dall'articolo 8 al fine di comprendere al meglio come esso operi concretamente.

presente regolamento. [...]». Quest'ultimo considerando relativamente al consenso sancisce che esso una volta espresso in maniera conforme, rimane nel tempo per consentire al titolare del trattamento di proseguire il trattamento dei dati.

⁴⁷ I quali chiariscono le modalità di acquisizione del consenso, delle qualità che questo consenso deve avere affinché il trattamento dei dati sia lecito.

⁴⁸ Denominato: "Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione". Il quale stabilisce: «1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, 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. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni. 2. Il titolare del trattamento si adoperi in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili. 3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore».

⁴⁹ Sul punto tornerò *infra*

Secondo autorevole dottrina l'operatività di tale disposizione è fortemente limitata⁵⁰ sotto vari punti di vista⁵¹. Al fine di avere un quadro normativo europeo completo, occorre sottolineare la delicatezza della questione del consenso prestato dal minore rifacendoci a quanto dichiarato nel Considerando n.38 del GDPR⁵².

Sebbene la protezione specifica del minore in internet venga spesso richiamata nella normativa sovranazionale, come nel Considerando 38, il legislatore europeo ha ritenuto corretto stabilire che il consenso al trattamento dei dati rilasciato dal minore sedicenne sia giuridicamente identico a quello prestato da un maggiorenne.

Inoltre, sorgono perplessità in merito al fatto che il Regolamento abbia rimesso agli Stati membri la decisione della soglia di età necessaria per esprimere il c.d. "consenso digitale"⁵³, ovvero, di stabilire la soglia di età a partire dalla quale il minore diviene autonomo nel prestare il consenso al trattamento dei propri dati necessari a poter usufruire dei servizi della società

⁵⁰ Sul punto si veda quanto scritto da autorevole dottrina: «[...] applicandosi soltanto ai trattamenti: a) di dati comuni, non quindi sensibili, giudiziari o genetici; b) basati sul consenso, ossia per i quali l'interessato debba manifestare il proprio assenso. Di conseguenza, se il trattamento risulta fondato su un altro presupposto, la norma non si applica; c) correlati all'offerta diretta di servizi della società dell'informazione» di M.NEGRI, *Il consenso digitale del minore. La disciplina del GDPR e le scelte del legislatore italiano*, in *Cyberlaws*, 20 maggio 2019. Link: <https://www.cyberlaws.it/2019/consenso-digitale-minore/>. Ma si veda anche: G.FINOCCHIARO, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2017, p. 167

⁵¹ Non si deve dimenticare come l'offerta del servizio online debba essere realizzata esclusivamente nei confronti di minori. Infatti, se un prestatore di tali servizi specifica di erogare il servizio esclusivamente a maggiorenni, tale servizio non è considerato offerto a un minore e quindi l'articolo 8 non troverebbe applicazione.

⁵² "I minori meritano una specifica protezione relativamente ai 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. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore."

⁵³ E.MAESTRI, *La tutela dei minori nell'età del consenso digitale. Un approccio gius-cibernetico*, AIAF, 2019; I.A.CAGGIANO, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, Familia, 2018, F.1, pp.3-23

dell'informazione⁵⁴. Questa scelta del legislatore europeo rende *de facto* la normativa differente in ogni stato dell'Unione e di conseguenza non assicura un'omogeneità ed un'armonia legislativa nel trattamento dei dati dei minori che invece sarebbe necessaria anche al fine di esperire rimedi e tutele del minore stesso⁵⁵.

L'Italia, come è noto, ha deciso di conservare una propria normativa in materia di riservatezza dei dati, integrativo del regolamento europeo (decreto legislativo n.101 del 2018). Tale decreto nel modificare l'art. 2-quinquies del Codice della privacy⁵⁶ ha fissato la soglia d'età a 14 anni⁵⁷, abbassando quindi quella suggerita dall'art.8 par.1 del GDPR⁵⁸. Ne deriva, come appare evidente, un'incongruenza tra l'età minima poter scaricare l'app e la possibilità di utilizzarla. Infatti, un minore con un'età inferiore ai 14 anni ha bisogno del consenso degli esercenti responsabilità genitoriale per scaricare un'App ma non per iscriversi ad un *social network*⁵⁹. Allo stesso modo, un minore con

⁵⁴ Si ricorda che per "servizi della società dell'informazione" si deve intendere quanto sancito dall'art.1 par.1 della Direttiva 1535 del 2015 (cui rinvia l'art.4 par.25 del Regolamento): «qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi».

⁵⁵ La soglia d'età per il valido consenso del minore mutando da paese a paese all'interno dell'Unione europea creerebbe problemi anche di trattamento dei dati della stessa App ove il minore viaggiando nell'area Schengen scaricasse sul proprio dispositivo un'app locale o visitasse un sito internet prestando il consenso al trattamento dei suoi dati. Si veda anche sul punto autorevole dottrina: G.M. RICCIO, G. SCORZA, E. BELISARIO, *GDPR e Normativa Privacy*, Commentario, Ipsoa, 2018. In Europa, infatti, vige l'attuale situazione: Croazia, Germania, Lituania, Lussemburgo, Malta, Paesi Bassi, Romania, Slovacchia, Ungheria hanno lasciato la soglia a 16 anni. Grecia, Repubblica Ceca, Slovenia, Francia l'hanno abbassata a 15 anni. Austria, Bulgaria, Cipro, Lituania ed Italia hanno fissato tale soglia a 14 anni. Belgio, Regno Unito, Spagna, Svezia, Inghilterra, Danimarca, Estonia, Latvia, Lettonia, Finlandia, Polonia, Portogallo a 13 anni. Si veda la ricostruzione operata da B. SAETTA, *Minori e protezione dati personali*, Settembre 2018 consultabile al link: <https://protezionedatipersonali.it/minori-e-protezione-dati-personali>.

⁵⁶ D.lgs. 196/2003, art.2 quinquies denominato: "Consenso del minore in relazione ai servizi della società dell'informazione".

⁵⁷ Vedi il comma 1. Questa decisione che può sembrarci quantomeno discutibile è stata dettata anche dal fatto che come previsto dall'art. 7, co. 2, legge n. 184 del 1983 in tema di adozione: il minore di 14 anni esprime un valido consenso all'adozione. Di medesimo avviso il parere del 22 maggio 2018 del Garante Privacy: "incoerente ammettere il quattordicenne a prestare il proprio consenso per essere adottato, ma non per iscriversi a un *social network*".

⁵⁸ 16 anni.

⁵⁹ Ad esempio: Facebook ha come soglia minima d'età per l'iscrizione 13 anni.

un'età pari a 14 anni che può, quindi, scaricare liberamente un'App senza il consenso dei genitori potrebbe trovarsi nella condizione di non poter usare tale App, prevedendo essa un'età minima di 16 anni⁶⁰ per l'iscrizione. Se poi consideriamo che nei casi citati entrambe le App sono molto popolari ed appartengono alla stessa compagnia questo rappresenta ancor di più un punto su cui riflettere.

Allo stesso modo il Codice della Privacy impone altresì che il titolare del trattamento rediga il proprio documento di acquisizione del consenso con "linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore" (Art.2 *quinquies* c.2) al fine di ottenere dallo stesso un consenso "significativo" in merito al trattamento dei suoi dati. Il Legislatore nazionale ha previsto un obbligo di condotta in capo al soggetto che tratta i dati del minore.

In accordo con tale previsione l'art. 166 del Codice Privacy prevede che la violazione dell'articolo 2-*quinquies* comporti l'applicazione di una sanzione amministrativa molto severa⁶¹.

Tuttavia, la norma lascia ampi margini di interpretazione e di conseguenza un'amplissima autonomia alle imprese *high-tech* nel definire in concreto gli standard della *policy* necessari per l'acquisizione di un consenso "significativo" del minore di anni 14. Sembra, quindi, estremamente difficile configurarne con certezza la violazione.

Se, quindi, è evidente che un'App per essere scaricata su un dispositivo debba richiedere preventivamente un valido consenso, è altrettanto evidente come una volta scaricata al primo accesso per funzionare venga richiesta spesso una registrazione nella quale è necessario accettare *in toto* la *policy* che autoregola l'uso dell'App pena la non possibilità di utilizzo. Questo ultimo passaggio rende *de facto* il creatore dell'App l'unico soggetto che può disciplinare ed eventualmente sanzionare il comportamento dell'utente durante l'utilizzo dell'App senza doversi giustificare né motivando eventuali sanzioni. Aziende private che sono tenute autonomamente a fare un *check*

⁶⁰ WhatsApp ha come soglia minima 16 anni.

⁶¹ Sanzione che: "può giungere fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo, nei casi più gravi"

and balance dei diritti costituzionali degli utenti senza che lo Stato possa fare nulla⁶².

A conferma delle perplessità appena rilevate, nel 2016 la Commissione europea ha pubblicato un importante Rapporto mirante ad approfondire il comportamento dei minori online⁶³ relativamente alle pratiche di regolamentazione vigenti nel panorama europeo, nel quale è stato evidenziato che nella maggior parte degli Stati membri lo schema prevalente è quello della autoregolamentazione, mentre la co-regolamentazione è prevista solo in pochissimi paesi.

Inoltre, dall'analisi effettuata dalla Commissione è emerso che la *self-regulation*⁶⁴ «non dà sufficienti garanzie di protezione dei minori, in quanto, alla luce delle evidenze empiriche raccolte, non permette al bambino/adolescente una facile identificazione dei contenuti commerciali e dell'intento persuasivo dei relativi messaggi»⁶⁵.

⁶² Per comprendere la gravità della situazione, a parere di chi scrive è come se noi affidassimo un minore ad un istituto straniero il cui scopo non è la cura e la crescita del ragazzo come una persona con diritti e doveri ma come il consumatore ideale. Senza considerare che secondo autorevole dottrina vedi C. BISTOLFI, *L'età del "consenso digitale" e il delicato rapporto tra minori e sicurezza online*, in www.ictsecuritymagazine.com, 8 novembre 2017.: "negli Stati Uniti il *Children's Online Privacy Protection Act* fissa l'età del consenso digitale a 13 anni. A questo punto, i service provider con sede negli USA – la maggioranza – potrebbero escludere la fetta di utenti europei di età compresa tra i 13 e i 15 anni, per evitare di dover sviluppare sistemi di verifica del consenso genitoriale, o, peggio, potrebbero interrompere la fruizione del servizio nei Paesi non allineati alla soglia dei 13 anni, con evidente pregiudizio alla libertà di informazione e di accesso alla rete" concorde L. BOLOGNINI e C. BISTOLFI in *L'età del consenso digitale – Privacy e minori on line, riflessioni sugli impatti dell'art. 8 del Regolamento 2016/679 (UE)*, 7 marzo 2017, p. 11. e ripreso in *Il consenso digitale del minore. La disciplina del GDPR e le scelte del legislatore italiano*, Cyberlaws, Maggio 2019, di M.NEGRI: "semplici attività come mandare e-mail, caricare contenuti sulle piattaforme di sharing, condurre ricerche o acquistare prodotti online potrebbero essere compromesse, creando un *digital divide* che penalizzerebbe i ragazzi europei sprovvisti di una legge nazionale che fissi a 13 anni l'età del consenso digitale rispetto ai coetanei americani"

⁶³ Nello specifico, tra i 6 e i 12 anni, dal titolo: *Study on the impact of marketing through social media, online games and mobile applications on children's behaviour*.

⁶⁴ Prevista all'art.40 lett.g del GDPR e confermata nel Considerando n.77 come *best practice*.

⁶⁵ A conferma di tale affermazione si veda ad ultimo esempio il giudizio del Garante privacy in merito al caso TikTok disponibile ai link: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524224>; <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533424>

Nello studio sono stati indicati due possibili cambiamenti utili a poter introdurre miglioramenti nella tutela della privacy dei minori.

In primo luogo, il ricorso a schemi di co-regolamentazione, in secondo luogo, ed in subordine, prevedere un maggiore *empowerment* dei minori⁶⁶. A valle di quanto analizzato nel rapporto tra minori ed app in merito al consenso una soluzione prospettata da alcuni⁶⁷ potrebbe essere la c.d. *enforced self-regulation*⁶⁸. In base ad essa, i codici di condotta dovrebbero essere elaborati mediante negoziazioni con i soggetti interessati⁶⁹ in un approccio *bottom-up*. Gli impegni assunti a tutela dei minori da parte dei titolari e responsabili del trattamento in esito a tale procedimento potrebbero essere resi vincolanti con poteri sanzionatori attribuiti all'autorità di controllo⁷⁰. Tutto ciò al fine di

⁶⁶ Si noti qui il fatto che il rafforzamento delle capacità di comprensione dei codici di condotta è legato ai direttamente minori non ai loro genitori. Per ciò che concerne le misure di *empowerment*, le prescrizioni di cui all'art. 2-quinquies, comma 2 del Codice Privacy introducono una serie di obblighi molto significativi in capo al titolare del trattamento dei dati del minore, tesi a "rendere significativo il consenso". Come, ad esempio, stabilire un obbligo di information *disclosure*, ossia un obbligo informativo a carico del titolare del trattamento, al quale è obbligato a: «redigere le informazioni e comunicazioni relative al trattamento» che riguardano il minore. La ratio della norma si riferisce ad una semplificazione del linguaggio per il minore obbligando quindi il titolare ad adottare: a. un tipo di linguaggio chiaro e semplice, conciso ed esaustivo, e b. alla modalità di espressione dell'informazione, facilmente accessibile e comprensibile».

⁶⁷ Si ritiene necessario citare tra i molti e senza pretesa di completezza: T.MILOSEVIC, B.O'NEILL, E.STAKSRUD, *Narratives of Industry Responses to Cyberbullying: Perspectives on Self-regulation from and About the Industry*. in: H.VANDEBOSCH e L.GREEN, *Narratives in Research and Interventions on Cyberbullying among Young People*. Springer, Cham, 2019. W. JACQUI, *Social media: end self-regulation, say MPs in report on children's health*, BMJ, 2019; pp.364 : 1486. K.A. ERDMANN e S. HERTEL, *Self-regulation and co-regulation in early childhood development, assessment and supporting factors*. Metacognition Learning 14, pp.229-238 (2019), <https://doi.org/10.1007/s11409-019-09211-w>.

⁶⁸ Una forma di *co-regulation*. Per approfondimento sull'*enforced self-regulation* si rimanda a: J. BRAITHWAITE, *Enforced Self-Regulation: A New Strategy for Corporate Crime Control*. Michigan Law Review, vol. 80, no. 7, 1982, pp. 1466-1507.; D.A. HYTHA, J.D. ARONSON e A.ENG, *Technology Innovation and the Rebirth of Self-Regulation: How The Internet of Things, Cloud Computing, Blockchain, and Artificial Intelligence Solve Big Problems Managing Environmental Regulation and Resources*. International Journal of Communication, [S.l.], v. 13, p. 5, oct. 2019. N.D. WOODS, *The Limitations of Meta-regulation*, Journal of Public Administration Research and Theory, Vol. 29, 1, January 2019, pp. 152-155.

⁶⁹ L'industria *high tech*, le piattaforme digitali, l'Autorità garante per l'infanzia e l'adolescenza, le persone di minore età stesse, il Garante per la protezione dei dati personali e l'Agcom

⁷⁰ Concorde a questa ipotesi si pone in modo molto deciso il Consiglio d'Europa nella Raccomandazione sopra menzionata. nei punti 67 e 68, 77 e 100.

assicurare ai minori una tutela ad oggi rimessa completamente alla valutazione delle compagnie private⁷¹.

5. Normativa, dottrina e del comportamento dei minori sui social.

Autorevole dottrina⁷² ha evidenziato i rischi di una società sempre connessa per l'individuo. Ovviamente, per i minori questi rischi aumentano ed è proprio per questo motivo che la nostra Costituzione all'art.31 c.2 prevede che lo Stato: "protegge l'infanzia e la gioventù favorendo gli istituti necessari a tale scopo"⁷³. Articolo questo che va letto unitamente al principio di inviolabilità dei diritti fondamentali di cui all'art. 2 Cost. ed al principio di uguaglianza sostanziale art. 3, c. 2 Cost. al fine di spingere il legislatore ad adottare una disciplina volta a garantire gli interessi dei minori anche nel settore dei media⁷⁴.

⁷¹ Se ciò è vero in generale alcuni dubbi si acquisiscono se queste App hanno lo scopo di raccogliere e gestire dati medici di minori. Vedi ad esempio il dibattito suscitato dall'App Immuni al tempo del Covid-19 e le perplessità espresse dal il Comitato parlamentare per la sicurezza della Repubblica (Copasir) il 14 maggio 2020 ed il parere espresso il 29 Aprile 2020 dal Garante Privacy nel Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da Covid-19, registro dei provvedimenti n. 79.

⁷² S. RODOTÀ, *Tecnopolitica, la democrazia e le nuove tecnologie della comunicazione*, Roma, 1997, p. 151: "Siamo passati a un mondo di informazioni condivise con una pluralità di soggetti, dove il riferimento al valore in sé della persona e alla sua dignità diviene secondario rispetto alla trasformazione dell'informazione in merce".

⁷³ Il secondo comma dell'art. 31 Cost. recita che la Repubblica «protegge [...] la maternità, l'infanzia e la gioventù, favorendo gli istituti necessari a tale scopo». Per autorevole dottrina a sostegno della connessione fra art.31 e comunicazione si veda L. CASSETTI, *Art. 31*, in R. BIFULCO, A. CELOTTO, M. OLIVETTI, *Commentario alla Costituzione*, Torino, 2006.

⁷⁴ Per un approfondimento sul tema si lascia ad autorevole dottrina il compito di meglio far comprendere i concetti appena espressi. In particolare ci si riferisce a: F.DONATI, *La tutela dei minori nella direttiva 2018/1808*, *Medialaws*; l. 176/1991 ha ratificato la Convenzione internazionale sui diritti dell'infanzia e dell'adolescenza del 1989 il cui art. 3 sancisce che "In tutte le decisioni relative ai fanciulli, di competenza delle istituzioni pubbliche o private di assistenza sociale, dei tribunali, delle autorità amministrative o degli organi legislativi, l'interesse del fanciullo deve essere una considerazione preminente". Dall'art. 16 della medesima Convenzione in cui viene stabilito che "nessun fanciullo sarà oggetto di interferenze arbitrarie o illegali nella vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza e neppure di affronti illegali al suo onore e alla sua reputazione. Il fanciullo ha diritto alla protezione della legge contro tali interferenze o tali affronti". M.C. MAFFEI, *La tutela internazionale dei diritti del bambino*, in L. PINESCHI, *La tutela internazionale dei diritti umani*, Norme, garanzie, prassi, Milano, 2006, 232 ss.

Il periodo dell'adolescenza è sicuramente un periodo delicato in cui l'individuo va a formare la sua identità e la sua personalità che poi sarà alla base della sua evoluzione futura tramite l'espressività e la socializzazione⁷⁵. È pacifico affermare per tale motivo che i giovani, in questa fascia d'età, debbano essere particolarmente tutelati dal momento che, come già sottolineato, i *social* presentano la possibilità di una loro libera e volontaria iscrizione; spesso, senza che essi si rendano conto di entrare in una "piazza" virtuale⁷⁶.

⁷⁵ A tal riguardo vedi le teorie di psicologia dello sviluppo elaborate da Meltzer ed Erikson. Quest'ultimo in particolare sviluppa una teoria della personalità che integra in una prospettiva globale e unitaria le tappe dello sviluppo psicosessuale con i momenti pregnanti, nella storia dell'individuo, del processo di socializzazione. Erikson non pone l'accento sull'ES e sulla corrispondenza tra stati evolutivi e zone erogene, come nella concezione freudiana, ma sulle funzioni dell'Io-linguaggio, pensiero, azione, gioco e sulle tappe del processo di socializzazione. Questa prospettiva considera la persona non solo inserita nel nucleo familiare, ma anche nel contesto sociale e induce a considerare l'influenza che la situazione storico- culturale propria di una società esercita sull'individuo. Vedi link: <https://elementidipsicologia.wordpress.com/2013/12/18/lo-sviluppo-dellidentita-personale-erikson/> e R.GILLIBRAND, V.LAM, V.L.O'DONNELL *et al.*, *Psicologia dello Sviluppo*, Pearson, 2019.

⁷⁶ C'è anche chi considera Facebook un possibile attore del servizio pubblico d'istruzione C. Giannikas, *Facebook in tertiary education: The impact of social media in e-Learning*, Journal of University Teaching & Learning Practice, 2020. L'A. nel suo elaborato dimostra che: "The majority of the responses indicated that Facebook was more accessible and user-friendly for discussions and knowledge-sharing in an e-learning context. Students' familiarity with Facebook and its user-friendly interactive features made discussion activities more effective." In merito all'accesso a Facebook come diritto costituzionale si veda la decisione della Suprema corte USA nel caso *Packingham v. North Carolina*.

Piazza che per sua natura intrinseca è accessibile e può essere utilizzata da chiunque⁷⁷, rientrando a pieno titolo nei mezzi di diffusione del pensiero⁷⁸. Tutto ciò premesso, in dottrina alcuni⁷⁹ sostengono che «il periodo dell'adolescenza enfatizzi il ruolo delle tecnologie rispetto al processo di autodeterminazione», altri⁸⁰ che «in questa fase della crescita e dello sviluppo la tecnologia consente di attivare nuovi percorsi di ricerca e di esplorazione identitaria»⁸¹.

⁷⁷ Ad esempio: in questo, Facebook, come ogni altro social, si presenta come una grande piazza e luogo di socializzazione, tant'è che, come da sentenza della Cassazione Penale Sez. I del 12 settembre 2014 n. 37596, Facebook può essere considerato come un "luogo aperto al pubblico". nel quale si applicano regole contenute nelle policies delle piattaforme private che disciplinano dando un proprio contenuto, principi costituzionali quali libertà di manifestazione del pensiero, della segretezza della corrispondenza e di autodeterminazione sanciti rispettivamente dagli articoli 21, 15 e 2 della Costituzione. Si noti che per luogo aperto al pubblico si deve intendere: "qualsiasi luogo fisicamente separato dall'esterno, l'accesso al quale è regolato dalla parte di coloro che ne abbiano la disponibilità, che possono consentire l'accesso stesso in via del tutto libera ovvero a determinate condizioni" F. GAMBINI, *Art. 17*, in Commentario breve alla Costituzione, a cura di in S. BARTOLI e R. BIN, Padova, 2008, p.140. Sul punto anche altra autorevole dottrina: A.PAPA, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Giappichelli, 2009.

⁷⁸ A livello sovranazionale è importante ricordare come il diritto all'informazione e alla comunicazione sia riconducibile alla libertà di espressione ai sensi del primo comma dell'art. 10 della Convenzione di Roma del 1950 e che esso costituisce "un interesse fondamentale della persona umana". Allo stesso modo la libertà di espressione, sempre al livello sovranazionale, è altresì tutelata dall'art. 11 della Carta dei diritti fondamentali dell'Unione Europea del 7 dicembre del 2000. Tale diritto trova un limite invalicabile nella tutela della dignità della persona specie se minore di età. La Suprema Corte con sentenza 5 sett. 2006/19069 ha infatti affermato la necessità di tutela del minore nell'ambito del mondo della comunicazione: "i minori essendo soggetti deboli necessitano di apposita tutela, non avendo ancora raggiunto un'adeguata maturità ed essendo ancora in corso il processo relativo alla loro formazione".

⁷⁹ M.MARTONI, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, federalismi.it, 08/01/2020.

⁸⁰ A. GUARINI, S. M. E. NICOLETTI, F. ROGA *et al.*, *Internet e social: i ragazzi raccontano le possibilità e i rischi della rete*.

⁸¹ Queste affermazioni sono suffragate da studi scientifici che dimostrano lo stretto legame tra social e sviluppo della personalità dell'adolescente. Secondo lo studio di Schimt et alt. Condotta nel 2008 "li aiutano a far capire chi sono" (richiamato in A. GUARINI, S. M. E. NICOLETTI, F. ROGA et al., *Internet e social: i ragazzi raccontano le possibilità e i rischi della rete*, cit., p. 61). Da queste teorie dottrinali e filosofiche è nata 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. K.C. MONTGOMERY, *Youth and*

Si sta quindi assistendo allo sviluppo di una generazione in cui la doppia identità (virtuale e reale) si sta lentamente trasformando in un'unica identità virtuale. In una società dell'apparenza spesso la personalità dominante non sarà quella reale ma quella virtuale.

Questo fenomeno, che viene messo in luce ancora di più grazie alla *datafication*⁸², rappresenta uno dei rischi maggiori per i minori in quanto soggetti spesso inconsapevoli dei propri diritti e doveri⁸³.

Surveillance in the Facebook Era: Policy Interventions and Social Implications, in Telecommunications Policy, vol. 39, 2015, n. 9, pp. 771-786.

⁸² La *datafication*, o datificazione, si definisce come: il processo che permette la trasformazione delle attività umane in dati digitali rappresentati da sequenze di numeri. La datificazione ha avuto origine con la nascita dei primi social network e si sta rafforzando nei giorni nostri. Essa rappresenta qualcosa che non ha precedenti, la mole di dati, Anche detti Big Data, raccolti da utenti più o meno consapevoli ha di per sé un valore economico maggiore di ogni altro bene conosciuto. Si veda fra i molti: A. VAN 'T SPIJKER, *The New Oil: Using Innovative Business Models to turn Data Into Profit*; D. BUCKINGHAM, *Data is the new oil*; e CLIVE HUMBY, il quale ha affermato: "Data is the New Oil", February 9th 2019: «*Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value*». Per un approfondimento sulla nozione di datificazione si vedano fra i molti: V. BERLINGO, *Il fenomeno della datafication e la sua giuridicizzazione*, in Rivista trimestrale di diritto pubblico, 3, 2017, pp. 641 ss.; J. E. MAI, *Big Data Privacy: The Datafication of Personal Information*, in The Information Society, 32, 3, 2016, pp. 192-199; J. VAN DIJCK, *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in *Surveillance and Society*, 12, 2, 2014, pp. 197-208. Il governo britannico è stato il primo a suddividere le fonti dalle quali vengono attinti questi dati. Nel report: *Who knows what about me?* vengono distinti: i dati concessi direttamente c.d. *given directly* (necessari per l'iscrizione), i dati c.d. *given off* che sono tutti quei dati acquisiti dal social tramite cookies e attività online e questi includono anche i metadata, ad ultimo gli *inferred data*. Le aziende dell'high-tech e proprietarie dei social ricavano dai dati *given off* e dai metadata, gli *inferred data*. Infatti, i metadata provengono dall'utilizzo in senso stretto dell'app o del social quindi il postare una foto geolocalizzandola, oppure il tempo passato online sul social ecc. mentre gli *inferred data* provengono da un'analisi dei *given off* e dei *given directly*. L'analisi viene fatta generalmente tramite machine learning e grazie ad Intelligenze Artificiali sempre più in grado di profilare l'utente automaticamente. Si Veda: Children Commissioner's Office, *Who knows what about me?*, 2018, p. 6 nota 9 e si veda: il report dell'Information Commissioner's Office (UK), *Big data, Artificial Intelligence, Machine Learning and Data Protection*, pubblicato il 4 settembre 2017.

⁸³ Si veda sul punto lo studio fatto dall'autorità inglese sul rischio nel lungo termine della datafication di un minore: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automateddecision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/>.

La datificazione che sta avvenendo potrebbe anche pregiudicare l'entrata nel mondo del lavoro degli attuali adolescenti in quanto la richiesta di accesso al proprio profilo social per valutare

Un altro rischio che corrono i nativi digitali è legato ad un fenomeno tristemente in ascesa, il cyber-bullismo⁸⁴. Il problema maggiore è che dal punto di vista penale il cyberbullo infra-quattordicenne è sempre non imputabile e per le condotte perpetrate da un minore tra i 14 ed i 18 anni va dimostrata la sua piena capacità. In ogni caso le pene previste sono inadeguate così come i rimedi possibili previsti dalla legge⁸⁵.

Non bisogna dimenticare, infatti, che la velocità di diffusione sui *social* è altissima ed una volta che un contenuto è in rete può essere bloccato solo dopo ore e a volte solo tramite provvedimento giudiziario, che però elimina o meglio oscura il contenuto solo sul nostro territorio nazionale⁸⁶. Il diritto all'oblio che può sicuramente essere esercitato al momento presenta ancora molte lacune tecniche. Per ciò che concerne la responsabilità civile delle azioni del cyber-bullo minorenni i genitori o tutori avendo la responsabilità genitoriale art.2048 codice civile sono gli unici responsabili⁸⁷.

l'idoneità del candidato al posto offerto. Quest'ipotesi che può sembrare inverosimile è già una realtà negli USA; dove al fine di richiedere visti temporanei viene richiesto dal *Department of Homeland Security (DHS)*. Il DHS chiede: sulla propria piattaforma di dare il consenso per l'accesso da parte dell'Autorità al proprio profilo social giustificando questa richiesta con lo scopo di valutare al meglio l'idoneità dell'individuo ad entrare nel paese.

⁸⁴ Per la definizione offerta dal legislatore nazionale vedi: L. n. 71 del 2017 definisce cyber-bullismo: "qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo". Per un approfondimento sul tema si rinvia a P.ARGANELLI, *Il Cyber-bullismo: un nuovo fenomeno in ascesa*, Rivista online Diritto Mercato e Tecnologia, www.dimt.it, 2017.

⁸⁵ L'unica eccezione a quanto appena affermato è rappresentata dai casi in cui il cyberbullismo è legato a reato più grave. La Cassazione penale sez. V, 27/04/2017, n.28623, stabilì che: "È configurabile il reato di stalking in caso di bullismo".

⁸⁶ Volendo fare un esempio se venisse pubblicato un video su un social ritraente la vittima del cyber-bullo occorrerebbero ore prima che il post possa essere rimosso, in queste ore il video potrebbe diventare virale e sconfinare il territorio rimanendo *de facto* in rete per sempre. Si veda tra le altre la sentenza: "Google-Vivi down" Cass. pen. sent. n. 5107/13.

⁸⁷ La giurisprudenza sul punto è numerosa, qui l'autore ritiene opportuno citare quanto sancito dalla Cassazione civile sez. III, 10/09/2019, n.22541: «*l'età ed il contesto in cui si è verificato il fatto illecito del minore non escludono né attenuano la responsabilità che l'art. 2048 c.c. pone a carico dei genitori, i quali, proprio in ragione di tali fattori, hanno l'onere di impartire ai figli l'educazione necessaria per non recare danni a terzi nella loro vita di relazione, nonché di vigilare sul fatto che l'educazione impartita sia adeguata al carattere e alle attitudini del*

minore, dovendo rispondere delle carenze educative cui l'illecito commesso dal figlio sia riconducibile». Si veda anche quanto sancito dal Tribunale minorenni di Caltanissetta, 10/07/2018 la quale ha affermato che i genitori sono responsabili civilmente anche in caso di divulgazione di foto intime da parte del minore e procedimento ex art. 333 c.c. avverso i genitori. Consultabile in *Diritto di Famiglia e delle Persone (II)* 2019, 2, I, 668. La sentenza può leggersi anche in *ilfamiliarista.it.*, con nota di C. RAVERA, *Minori e internet: quando i genitori devono vigilare*. Per un approfondimento in tema di divulgazione di foto personali intime da parte di minori, si veda M. BIANCA, A. GAMBINO, R. MESSINETTI, *Libertà di manifestazione del pensiero e diritti fondamentali. Profili applicativi sui social networks*, Milano, 2016; M. MONTANARI, *La responsabilità delle piattaforme online (Il caso Rosanna Cantone)*, in *Dir. inf.*, 2017, 254 ss.; V. VENTURA, *Non può dirsi "utilizzato" il minore che diffonda il proprio autoscatto a carattere pornografico*, in *Ilpenalista.it*, 2016; M. ALOVISIO, *Il selfie: la cessione online di materiale pedopornografico prodotto dal minore stesso*, in *Dir. giust.*, 2016, 42 ss. In senso conforme alla massima, in giurisprudenza, Cass. 5 settembre 2006 n. 19069, in *Dir. giust.*, 2006, 36, con nota di San Giorgio; Trib. Teramo 16 gennaio 2012 n. 18, in *Dejure.it*. Sulle responsabilità penali della divulgazione di fotografie intime, v. Cass. pen. 26 settembre 2018 n. 1923, in *Dir. giust.*, 17 gennaio 2019; GIP La Spezia 30 giugno 2016 n. 971, in *Dejure.it*; Cass. pen. 26 marzo 2013 n. 19033, in *CED Cass. pen.*, 2013; Cass. pen. 5 febbraio 2009 n. 10085 in *Dejure.it*; Cass. pen. 15 febbraio 2008 n. 14230 in *Dejure.it*. Con riguardo alla necessità di "educazione ai social media", si veda il recente contributo di V. GHENO e B. MASTROIANNI, *Tienilo acceso*, Milano, 2018. Ad ultimo si ritiene importante citare il Tribunale Sulmona, 09/04/2018, secondo cui devono ritenersi civilmente responsabili, ex art. 2048, comma 1, c.c., i genitori di soggetti minorenni che diffondano, utilizzando mezzi telematici (WhatsApp, Facebook, etc.), fotografie contenenti l'immagine nuda di una coetanea e siffatta diffusione avvenga senza il consenso dell'interessata, in quanto è ad essi ascrivibile la culpa in vigilando ed in educando. In quest'ultimo caso secondo il Tribunale di Sulmona afferma che: «la responsabilità parentale può essere esclusa, ai sensi del comma 3 dell'art. 2048 c.c., soltanto qualora i genitori dimostrino di non aver potuto impedire il fatto, dovendosi con ciò intendere che gli stessi abbiano integralmente adempiuto al dovere di educare la prole attraverso lo sviluppo nella stessa di una adeguata capacità critica e di discernimento. La circostanza che al momento della commissione dell'illecito la fotografia in oggetto fosse già diffusa all'interno della comunità di appartenenza del soggetto fotografato e che ciò fosse dovuto, tra l'altro, alla condotta disinibita tenuta dal soggetto stesso, attenua la responsabilità civile, ma non la esclude, configurandosi in capo alla persona ritratta, ed ai genitori della stessa, un danno non patrimoniale consistente nella lesione di una pluralità di interessi costituzionalmente protetti, tra cui il diritto alla riservatezza, alla reputazione, all'onore, all'immagine, all'invulnerabilità della corrispondenza». Ad ultimo è necessario citare per completezza le sentenze pronunciate dalla Cassazione civile sez. VI, 04/10/2019, n.24907 e Cassazione civile sez. III, 19/02/2014, n.3964 le quali, allargando ulteriormente il campo della responsabilità civile dei genitori verso la condotta dei figli, affermano che la responsabilità dei genitori è da attribuirsi anche per quei fatti legati alla condotta del minore avente una maturità che ne permetterebbe l'accertamento della piena capacità di intendere e di volere. Il tipo di esperienza che l'adolescente può fare in un social è quindi molteplice.

6. Il complesso bilanciamento tra *policies* private e diritti fondamentali.

Le scelte operate dai vari social media riguardo alle *policies* si scontrano spesso con i diritti e le tutele costituzionali dei cittadini del paese in cui il *social network* opera. Ogni paese europeo, infatti, come visto in precedenza, stabilisce un'età valida per prestare il consenso per scaricare le App e per utilizzarle differente e prevede tutele giuridiche diverse. Questo crea lacune nella tutela dei diritti degli individui che la giurisprudenza talvolta cerca di colmare.

Si pensi, ad esempio, come già accennato in precedenza alla *datification* rispetto al diritto alla tutela dell'identità personale e al diritto all'oblio⁸⁸.

The right to be forgotten sancito anche nel recente GDPR e relativa legge di recepimento del maggio 2018 è fondamentale per assicurare ai cittadini il rispetto dei diritti inviolabili previsti dall'art.2 della Costituzione; in quanto, come attentamente sostenuto:

«il carattere tendenzialmente imperituro dei dati immessi in rete e la crescente compenetrazione tra dimensione virtuale e vita reale ha, infatti, irrimediabilmente modificato il percorso evolutivo della personalità dei consociati, rendendo necessaria l'individuazione di nuove forme di tutela dell'identità della persona»⁸⁹.

Certamente questi dati presenti nei *social* rimangono finché il proprietario stesso non decida di cancellarli. Fino all'emanazione della sentenza *Google-Spain*⁹⁰ e successivamente con l'entrata in vigore del GDPR questo risultava

⁸⁸ Per approfondire il tema del diritto all'oblio si suggerisce: D. MESSINA, *Il diritto all'oblio tra vecchie e nuove forme di comunicazione e di espressione*, in Quaderni di Diritto Mercato Tecnologia, Anno VI, n. 3, 2016.

⁸⁹ D.MESSINA, *Diritto all'oblio e limite territoriale europeo: la sentenza della Corte di Giustizia UE C-507/17 del 24 settembre 2019*, *De Iustitia*, 2019. La *datification* è un fenomeno che colpirà maggiormente i nativi digitali ma è evidente come anche adesso riguardi un gran numero di utenti. Facebook, ad esempio, ripropone nel tempo "i ricordi degli utenti" a distanza di anni, utenti che un po' per mancanza di voglia, un po' per incapacità tecnica non sono in grado di gestire i dati pubblicati negli anni ed archiviati prontamente a fini commerciali.

⁹⁰ Corte di giustizia dell'Unione europea (CGCE), Causa C-131/12: GOOGLE SPAIN SL e GOOGLE INC. contro L'AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS E MARIO COSTEJA GONZÁLEZ.

altamente complesso se non impossibile⁹¹. Il nuovo GDPR grazie all'introduzione del diritto all'oblio permette di chiudere l'account, cancellare tutti i propri dati e salvarli offline sul proprio dispositivo. Sfortunatamente anche questo istituto così prezioso per difendere i propri diritti incontra una serie di limiti⁹² territoriali e temporali.

È opportuno sottolineare come ad oggi le *policies* applicando algoritmi più o meno complessi influenzino durante l'utilizzo dell'App i diritti fondamentali dei minori, i quali non possono far altro se non rinunciarvi in tutto o in parte per utilizzare tale App.

7. Il ruolo dello Stato italiano e dell'Europa nella protezione dei dati dei minori.

Nel panorama normativo appena descritto, se è vero che il nuovo Regolamento Europeo 679/2016, gli articoli 7 e 8 della Carta dei diritti fondamentali dell'U.E e le recenti decisioni della Corte di Giustizia⁹³ hanno "blindato" il diritto di ogni individuo a far rispettare la propria privacy, e a poter gestire i propri dati archiviati sui social media in senso teorico, è pur vero che da un punto di vista programmatico, viste le *policies* dei vari *social* è complesso far rispettare i propri diritti e molto spesso si può raggiungere l'obiettivo solo con delle azioni legali che se per le *high-tech companies* non sono particolarmente dispendiose mentre lo possono diventare per un singolo cittadino.

Tuttavia, sembra essersi rafforzato recentemente il ruolo dei tribunali nello spazio europeo nella tutela dei diritti dei cittadini. Si veda a tal proposito la

⁹¹ Pensiamo ad una coppia che stando insieme per anni pubblica centinaia di foto, ad un certo punto si lasciano, i profili di entrambi dovrebbero essere ripuliti da ognuno per anni ed anni indietro nel tempo. Foto per foto, video per video, post per post. Una mole di lavoro notevole con la spada di Damocle che in caso si dimentichi uno dei post si possa incorrere in un'azione da parte dell'ex partner. Infatti, se alcuni ricordi possono essere piacevoli altri possono non esserlo ed anzi ledere l'immagine o la reputazione del soggetto stesso o di altri a lui associati all'epoca.

⁹² Per approfondire i limiti del diritto all'oblio si rimanda ad autorevole dottrina: D. MESSINA, *Il diritto all'oblio tra vecchie e nuove forme di comunicazione e di espressione*, in Quaderni di Diritto Mercato Tecnologia, Anno VI, n. 3, 2016. D.MESSINA, *Diritto all'oblio e limite territoriale europeo: la sentenza della Corte di Giustizia UE C-507/17 del 24 settembre 2019*, De Iustitia, 2019, ISSN 24215414.

⁹³ Vedi Corte di Giustizia 131/12

recente sentenza della Corte di Giustizia Europea sez. III, 03/10/2019, n.18, la quale stabilisce che il provider, al fine di tutelare i diritti della vittima sanciti dall'art.18 della Direttiva del 08/06/2000 N. 31, è obbligato ad operare un filtraggio globale e specifico di contenuti equivalenti⁹⁴. Questa sentenza è di notevole interesse anche per quanti minori vittime di cyber-bullismo possono tramite una sentenza nazionale assicurarsi che i suoi effetti siano globali e grazie al prefiltraggio possano essere definitivi. Al contrario si rischierebbe un aggiramento delle sentenze dei tribunali nazionali ed una grave mancanza di tutela delle vittime che si troverebbero sempre a dover fare nuove azioni al fine di tutelare i propri diritti⁹⁵. Ad ultimo, sempre a livello europeo, l'art.10 della direttiva U.E. 2018/1808 ha introdotto il nuovo art.6bis c.2 della Direttiva SMAV il quale ha stabilito per le nuove piattaforme di diffusione dei contenuti audiovisivi (esempio i social media) il divieto di utilizzare per scopi commerciali i dati personali dei minori raccolti o altrimenti generali dai fornitori di servizi.

Si può affermare che sia le Corti italiane che quelle europee stanno costantemente lavorando per tutelare i diritti dei minori ed i loro dati, è giusto sottolineare il ruolo dello Stato italiano nel contrastare tali fenomeni grazie a progetti che mirano a divulgare le *best practices* e quindi la prevenzione dei

⁹⁴ La sentenza, infatti, fornisce un'interpretazione estensiva dell'art.15 par.1 della Direttiva 08/06/2000 - N. 31, il quale stabilisce che i singoli tribunali nazionali possono: «1.ordinare a un prestatore di servizi di hosting di rimuovere le informazioni da esso memorizzate e il cui contenuto sia identico a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, qualunque sia l'autore della richiesta di memorizzazione di siffatte informazioni; 2.ordinare a un prestatore di servizi di hosting di rimuovere le informazioni da esso memorizzate e il cui contenuto sia equivalente a quello di un'informazione precedentemente dichiarata illecita o di bloccare l'accesso alle medesime, purché la sorveglianza e la ricerca delle informazioni oggetto di tale ingiunzione siano limitate a informazioni che veicolano un messaggio il cui contenuto rimane sostanzialmente invariato rispetto a quello che ha dato luogo all'accertamento d'illiceità e che contiene gli elementi specificati nell'ingiunzione e le differenze nella formulazione di tale contenuto equivalente rispetto a quella che caratterizza l'informazione precedentemente dichiarata illecita non siano tali da costringere il prestatore di servizi di hosting ad effettuare una valutazione autonoma di tale contenuto; e 3. ordinare a un prestatore di servizi di hosting di rimuovere le informazioni oggetto dell'ingiunzione o di bloccare l'accesso alle medesime a livello mondiale, nell'ambito del diritto internazionale pertinente».

⁹⁵ Per un approfondimento della sentenza si veda: D. BIANCHI, *Diritto & Giustizia*, fasc.179, 2019, pag. 3, note a sentenza.

fenomeni di cyber-bullismo, furto d'identità e illeciti a danni o causati da minori. Questo avviene grazie a progetti nazionali, regionali e locali che coinvolgono reti di scuole di diversa estrazione socioculturale e portano degli esperti privati, esponenti delle forze dell'ordine e della magistratura a svolgere conferenze e lezioni sui temi relativi ai diritti dei cittadini ed a quelli dei minori in Internet⁹⁶.

8. Prospettive regolatorie per le sfide in atto e che verranno.

Nei precedenti paragrafi si è cercato di analizzare senza pretesa di completezza l'uso dei *social network* e delle App da parte di soggetti minori ed il ruolo che gli stessi nuovi media giocano nella loro crescita e formazione. Dall'analisi si può desumere che al momento, per ognuno degli aspetti analizzati, l'attuale normativa presenta una o più perplessità: lacune, difficoltà applicative, non comprensione dei cittadini sia maggiorenni che minorenni dei diritti e dei doveri espressi nella piazza virtuale della rete, bilanciamento tra le norme costituzionali lasciate alla libera interpretazione di

⁹⁶ Si pensi ad esempio fra i molti progetti realizzati dall'ente ANCEI Formazione e Ricerca www.ancei.org negli ultimi 5 anni grazie ai fondi del Ministero dell'Istruzione Università e Ricerca, della varie Regioni e della Presidenza del Consiglio dei Ministri: al progetto del 2018 "70 anni di Costituzione: i valori di cittadinanza, legalità e democrazia nei giovani dell'era 3.0." realizzato in partenariato con l'Istituto Via Gramsci di Valmontone oppure nello stesso anno il progetto: "La Carta dei diritti in alternanza scuola-lavoro: uno strumento di qualificazione dei percorsi, un'opportunità per il futuro degli studenti" realizzato in partenariato con l'Istituto Paolo Baffi di Fiumicino. Nel 2017 il progetto "Giovani Cittadini Protagonisti: Percorsi Educativi sulla Legalità e sulla Cittadinanza Attiva per Gli Adulti Di Domani" realizzato con l'Istituto Galilei di Roma; il progetto: "Cultura della Legalità per un'educazione efficace giovani cittadini" realizzato con Istituto Vespucci di Roma; il progetto: "Educazione al rispetto, stop alla Violenza Sessuale e di genere, al bullismo ed al cyberbullismo" realizzato con Istituto Paritario Maria Consolatrice di Roma; il progetto "R.I.V.A. Rete Integrata contro ogni Violenza, lontano dagli stereotipi per il rispetto reciproco" con Istituto Paritario Bonifacio VIII e Comune di Anagni. Nel 2015, il progetto "Promozione della cultura scientifica e valorizzazione del sistema di trasferimento tecnologico" in partenariato con gli istituti scolastici: ITAS Garibaldi di Roma, IIS Pertini di Genzano (RM), Liceo Scientifico Avogadro di Torino, Liceo Scientifico Maria Consolatrice Milano, Liceo Scientifico Internazionale Leoniano di Anagni (FR), IISS "Giordano" di Venafrò (IS), Liceo Scientifico Vailati di Genzano (RM) ed in collaborazione con il Università "La Sapienza" di Roma, facoltà di Ingegneria, Dipartimento DICEA.

soggetti privati ecc.: tutte problematicità evidenziate da tempo e conosciute nelle sedi istituzionali⁹⁷.

La pluralità dei legislatori e la loro interrelazione con il carattere sovranazionale delle imprese *high tech* rende impossibile un'univocità informativa⁹⁸ nonostante le numerose richieste pervenute in tal senso⁹⁹.

Tuttavia, è opinione condivisa che per affrontare e risolvere le questioni di cui si è dato conto nel presente lavoro occorra l'emanazione da parte del legislatore nazionale e/o europeo di una nuova normativa di riferimento che consenta da un lato una maggiore regolazione dei fenomeni che vedono come soggetti i minori nel mondo dei social network a sostituzione del quadro di *soft law* e dall'altro di colmare quelle "zone grigie" causate dalle differenze di tutela del minore nei vari paesi europei conseguenti ad una disomogeneità normativa attualmente presente.

Da troppo tempo la rete e le piattaforme digitali da essa nate non sono state oggetto di opportuna regolamentazione sovranazionale ma al contrario sono

⁹⁷ Si fa riferimento al IV Rapporto di aggiornamento 2007-2008, p.48-49, elaborato dal gruppo di Lavoro per la Convenzione ONU sui diritti dell'infanzia e dell'adolescenza, il quale già all'epoca sollevò il problema nel merito riguardante "la sicurezza per gli utenti più piccoli, poiché sono tra i principali fruitori e produttori di contenuti" (audiovisivi) e con riguardo ai *social network*, in cui il Gruppo di lavoro evidenziò come, sebbene questi consentano la piena libertà di espressione e comunicazione emergono comportamenti preoccupanti quali: "una scarsa attenzione ai propri dati personali e la propensione ad incontrare – non accompagnati– offline, persone conosciute in rete".

⁹⁸ A seguito del rapporto in nota precedente, il Parlamento italiano elaborò la proposta di un "Codice Unico Minori e Media" che includesse maggiori tutele per i minori non solo legate ai contenuti audiovisivi presenti sui "vecchi" canali di informazione e comunicazione ma anche e soprattutto su quelli nuovi dei social. La proposta purtroppo non fu mai trasformata in legge.

⁹⁹ Significativi a tal proposito sono i numerosi rapporti del Gruppo di Lavoro per la Convenzione ONU sui diritti dell'infanzia e dell'adolescenza che hanno richiesto al legislatore di fornire le autorità pubbliche di "adeguati strumenti sanzionatori di monitoraggio rispetto a TV, videogiochi, internet e cellulari". Per approfondimenti si suggeriscono: il II Rapporto supplementare 2009, ad p. 56; l'VIII Rapporto di Aggiornamento 2014-2015, ad p. 62.; il IX Rapporto di Aggiornamento 2015-2016, ad p. 71 ed ultimo in ordine cronologico il III Rapporto supplementare 2017, ad p. 74.

state lasciate all'autoregolamentazione pura (c.d. *self-regulation*¹⁰⁰) con tutte le conseguenze¹⁰¹ descritte¹⁰².

Se le notizie importanti, fondamentali per un paese, devono passarvi quasi obbligatoriamente per essere diffuse è evidente che quel *social network* svolge un servizio pubblico di informazione e come tale dovrebbe essere regolato.

Secondo alcuni¹⁰³ una possibile soluzione intermedia, in attesa del legislatore nazionale, pur prospettata da molti, potrebbe essere quella di passare da una *self-regulation* ad una *co-regulation*¹⁰⁴.

¹⁰⁰ In tal senso possiamo vedere quanto previsto all'art.40 par.2 lett.g del GDPR: «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 [...] 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». In altre parole, il GDPR ed il relativo Working Party hanno dimostrato di essere favorevoli ai codici di condotta scelti da parte delle industrie e quindi ai mezzi di autoregolamentazione. Tuttavia, l'adozione di un codice di condotta è facoltativa per l'azienda e la responsabilità rimane in capo al genitore/ esercente patria potestà. Infatti, gli articoli 58 par.2, 83 par.2 lett.j e 83 par.4 del GDPR stabiliscono che in caso di violazioni di cui all'art.8 il possedere un codice di condotta rappresenta "uno degli elementi da tenere in considerazione" nel decidere l'ammontare della sanzione amministrativa."

¹⁰¹ Si veda *infra* per approfondire i risultati dello studio svolto dalla commissione europea nel 2016 dal quale si evidenzia che negli stati europei che hanno adottato il modello della *self-regulation* i minori sono sostanzialmente meno tutelati: Commissione Europea, *Study on the impact of marketing through social media, online games and mobile applications on children's behaviour*, 2016 consultabile al link: https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrensbehaviour_en.

¹⁰² Senza contare che gli standard dei codici di condotta adottati dai social, a cui il minore presta il consenso per l'utilizzo dell'app o del software, sono a discrezione dell'azienda con l'unico limite di essere comprensibili al fine di assicurare al minore di comprenderne il contenuto.

¹⁰³ F. DI PORTO, in *La libertà di espressione del minore e il diritto all'accesso ai mezzi di comunicazione e alla riservatezza*, in *La Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza – conquiste e prospettive a 30 anni dall'adozione*, 2019, pag.230 e ss.

¹⁰⁴ Per una definizione di *co-regulation* si vedano tra i molti autorevoli: I. AYRES e J. BRAITHWAITE, *Responsive Regulation*, Oxford, 1994; R. BALDWIN, M. CAVE, M. LODGE, *Understanding Regulation*, Oxford University Press, 2012, p. 146). Essi la definiscono come "la definizione delle regole da parte delle associazioni dell'industria con qualche forma di controllo o ratifica da parte del soggetto pubblico: concretamente una *self-regulation* con in aggiunta il controllo più o meno permeante ed invasivo del Governo o del Parlamento. Alcuni, come la Prof.ssa F. DI PORTO, in *La libertà di espressione del minore e il diritto all'accesso ai*

Questa evoluzione si rende necessaria vista la sempre maggiore personalizzazione dei servizi dell'informazione, resa possibile dal continuo progresso tecnologico che ha dato vita al *machine learning* e all'intelligenza artificiale per la raccolta e lo sfruttamento dei dati. La *co-regulation* potrebbe portare a *policies* più comprensibili per un minore e soggette in caso di violazione ad un più facile processo di accertamento e sanzione da parte dell'autorità pubblica di controllo¹⁰⁵.

Se è vero che i *big data* sono il nuovo petrolio, il favorire la nascita di un social network europeo i cui dati raccolti vengano archiviati in Europa permetterebbe sia di risolvere i problemi relativi alla tutela dei dati personali in vita e superando la territorialità dei giudizi e dei provvedimenti nazionali, la loro applicabilità, la velocità di risposta della piattaforma ed inoltre consentirebbe l'adeguamento delle *policies* alla normativa europea e di rafforzare l'economia europea.

Se questa può sembrare un'idea troppo radicale, l'alternativa più plausibile è una riforma sostanziale della direttiva europea 31/2000/CE sull'e-commerce che modifichi la responsabilità delle piattaforme rispetto ai contenuti in esse immesse dagli utenti così come avvenuto recentemente con la direttiva UE 2018/1808 in materia di servizi media audiovisivi che hanno esteso la tutela del minore, riservata precedentemente alla TV, ai servizi erogati anche su internet.

mezzi di comunicazione e alla riservatezza, nov.2019, pag.230 suggerisco di utilizzare un modello c.d. "*enforced-self-regulation*" come "esempio di *co-regulation* che prevede il coinvolgimento del soggetto pubblico non tanto (o meglio, non solo) nella fase di definizione delle regole, ma soprattutto in quella di attuazione delle stesse.". La *co-regulation* viene anche appoggiata dallo studio della Commissione Europea del 2016 precedentemente citato, in quanto essa garantisce un maggior *empowerment* dei minori rendendo la loro *awareness* e capacità di gestione dei dati più attenta e migliore.

¹⁰⁵ Se infatti esse fossero frutto di negoziazione con tutti gli *stakeholders*, gli impegni assunti a tutela dei minori da parte dei titolari e responsabili del trattamento in esito a tale procedimento potrebbero essere resi vincolanti con decisione regolatoria. Di conseguenza, le autorità di controllo quali Agcom, Garante Privacy e Garante Adolescenza potrebbero avere dei veri poteri sanzionatori nel caso di violazione degli impegni volontariamente assunti. Concorde con questo sistema fu il Consiglio d'Europa nella Raccomandazione ai punti 67 e 68, 77 e 100: *Committee of Ministers of the Council of Europe, Guidelines to respect, protect and fulfil the rights of the child in the digital environment* (CM/Rec(2018)7), del 4 luglio 2018, consultabile al link: www.coe.int/en/web/children/the-digital-environment.

In questo modo, forse, si potrebbero spingere le piattaforme dei *social networks* ad eliminare tutta una serie di problematicità nel loro stesso interesse al fine di evitare possibili azioni legali degli utenti.

In conclusione, vista la situazione attuale, un primo passo dovrebbe essere fatto dagli stati nazionali e tra questi quello italiano per disciplinare la materia limitando l'autoregolazione e favorendo la co-regolazione al fine di giungere ad un codice unico in materia di minori ed internet come prospettato nel IV Rapporto di aggiornamento 2007-2008, elaborato dal gruppo di Lavoro per la Convenzione ONU sui diritti dell'infanzia e dell'adolescenza¹⁰⁶. Questo tipo di fonte, infatti, consentirebbe l'applicazione dei principi costituzionali direttamente da parte del legislatore nazionale e non da enti privati in regime di autoregolamentazione pura.

La nuova sfida del diritto contemporaneo è aperta.

¹⁰⁶ Il quale parlava di "Codice Unico Minori e Media", per un approfondimento sul contenuto del rapporto si veda *infra*. Si noti che il "codice di autoregolamentazione Tv e Minori" del 2002 ebbe inizialmente la forma di atto privato, fu poi recepito e trasformato con la legge di sistema n.112/04, trasfusa nel Testo Unico di cui al Decreto legislativo n.177/05, e successivamente modificato dal D.lgs n.44/10. Il Codice è divenuto vincolante per tutte le emittenti a prescindere dalla sottoscrizione dello stesso e dalla tipologia di piattaforma utilizzata. Esso rappresenta un esempio di come un codice di autoregolamentazione privato possa essere trasformato in legge per garantire equamente e uniformemente i diritti dei minori. Da notare che nel 2019 è stato proposto un D.D.L.: "Norme per la tutela dei minori che accedono alla rete internet e istituzione del registro dei provider aderenti al codice di autoregolamentazione Internet e minori", XVIII Legislatura, in Atti parlamentari del Senato della Repubblica n.1329, che si pone l'obiettivo di riformare ulteriormente il sistema.