NUOVE NORME ITALO-EUROPEE A TUTELA DEI MINORI ONLINE*

NEW ITALIAN AND EUROPEAN REGULATIONS REGARDING CHILDREN ONLINE PROTECTION

Alessia Valongo**

1 DALL'ESPERIENZA DI AUTOREGOLAMENTAZIONE AL MODELLO DI CO-REGOLAZIONE A TUTELA DEI MINORI *ONLINE*

Nell'ultimo trentennio, il complesso normativo in materia di tutela dei minori *online* si è notevolmente arricchito ed è tuttora in continua evoluzione, dal momento che l'autoregolamentazione non è stata in grado di governare, da sola, uno spazio così esteso come quello delle piazze virtuali. Fino agli anni 2000, nell'ambito della disciplina normativa è prevalso in Italia e nell'Unione Europea un approccio basato esclusivamente su meccanismi di *soft law* o di “diritto mite” (Zagrebelsky, 1992) a protezione dell'infanzia, su forme di *self-regulation*, ove i poteri regolatori vengono esercitati da enti non statali, di natura privatistica. Si fa riferimento soprattutto a codici di condotta emanati da professionisti della comunicazione, a codici di autodisciplina adottati da singole imprese digitali o da associazioni di categoria e, perciò, a regole capaci di cogliere le peculiarità del settore, provenendo proprio da coloro che, facendo parte di quel settore, possiedono le necessarie competenze tecniche per disciplinarlo in modo agile e flessibile (Bellelli, 2023).

Il primo esempio di tale approccio è rappresentato dalla Carta di Treviso, un Protocollo di intesa, firmato il 5 ottobre 1990 dall'*Ordine professionale dei giornalisti*, dalla *Federazione nazionale della stampa italiana* e da *Telefono Azzurro*, volto a disciplinare i

* Il lavoro si inserisce nell'ambito del Progetto *Visiting Valongo/Colombo* finanziato e rientra tra le attività del PRIN 2020 dal titolo: *E-Agorà - Online Platform Contracts: economic efficiency and rights' protection of service users. Technological innovation and service sharing in a social world*, del quale l'autrice è responsabile per l'Unità locale dell'Università degli Studi di Perugia. Il saggio è il risultato dell'arricchimento dottrinale e giurisprudenziale e dell'aggiornamento normativo di una relazione tenuta al Convegno su *Profili di (auto)regolamentazione delle piattaforme digitali*, svoltosi il 25 gennaio 2024, presso il Centro di Studi e Ricerca *Legalità e Partecipazione* (LEPA) del Dipartimento di Scienze Politiche dell'Università degli Studi di Perugia.

** Professoressa associata di Diritto privato presso il Dipartimento di Scienze Politiche dell'Università degli Studi di Perugia, Italia. È autrice di quattro monografie, la prima sulla soggettività giuridica del concepito, la seconda in tema di rimedi contrattuali, la terza sulle nuove genitorialità nel diritto delle tecnologie riproduttive e la quarta in tema di autonomia negoziale procedimentale e contratto preliminare. Tra le pubblicazioni su riviste nazionali e internazionali si segnalano vari saggi e contributi, anche in lingua inglese, in materia di diritti fondamentali delle persone, di diritto delle famiglie e dei minori, nonché in materia di obbligazioni, contratti e rapporti di consumo.

rapporti tra informazione e infanzia, sulla base di una concertazione tra le parti interessate. La Carta di Treviso, estesa nel 2006 al giornalismo digitale e multimediale e divenuta dal 2016 parte integrante del *Testo unico dei doveri del giornalista*, impegna tutti gli operatori dell'informazione, anche *online*, a rispettare l'anonimato del minore che sia coinvolto in eventi di cronaca, come soggetto sia attivo che passivo, come vittima, a preservarne l'immagine e la dignità e ad usare tutte le precauzioni necessarie per evitare strumentalizzazioni da parte degli adulti.

L'esperienza italiana di *self regulatory* mostra che, intorno alla fine degli anni novanta, l'Unione Europea inizia a incoraggiare gli *Internet service providers* all'adozione di codici deontologici per la protezione dei minori *online*, incidendo così sulla loro elaborazione¹. Di qui la loro natura non esclusivamente privata, considerati i poteri di raccomandazione e di controllo della Commissione europea. Tali fonti autoregulatorie hanno alla base una formazione negoziale del diritto (Lipari, 1987; Piepoli, 1997), che proviene dalle forme organizzative della società civile, in quanto coinvolge le associazioni rappresentative dei soggetti interessati (piattaforme *online*, utenti, imprenditori, professionisti, consumatori). Di particolare rilievo è il *Codice di autoregolamentazione Internet e minori*, firmato il 19 novembre 2003 da AIIP (*Associazione Italiana Internet Providers*), ANFoV (*Associazione per la convergenza nei servizi di comunicazione*), Assoprovider (*Associazione Provider Indipendenti*), Federcomin (*Federazione delle imprese delle Comunicazioni e dell'informatica*) e dal *Ministro delle Comunicazioni, per l'Innovazione e le Tecnologie*. Inizialmente concepito come atto di natura meramente privata con valenza solo sul piano morale e sociale, esso ha trovato in un primo momento scarsa adesione da parte degli operatori. Successivamente, tale Codice è stato recepito dalla legge delega n. 112 del 3 maggio 2004, dal d.lgs. n. 177 del 2005 e dal d.lgs. 8 novembre 2021 n. 208 (TUSMA, *Testo unico dei servizi di media audiovisivi*), i quali, in tal modo, ne hanno riconosciuto l'efficacia propriamente giuridica, di autentica fonte del diritto². Occorre, peraltro, sottolineare che,

¹ Si vedano: Raccomandazione del Consiglio dei Ministri europeo del 24 settembre 1998 n. 98/560 (in www.europarl.eu.int); Piano pluriennale d'azione comunitario, adottato con Decisione n. 276/1999/CE, pubblicata in VACCÀ, 1999; Direttiva 2000/31/CE sull'*e-commerce*, sia il d.lgs.70/2003 di attuazione, rispettivamente all'art. 16 e 18, richiamano l'elaborazione di codici di condotta al fine di garantire la tutela dei minori nella contrattazione telematica.

² L'art. 42 del TUSMA, al comma 3, prevede che l'Autorità per le Garanzie nelle Comunicazioni, sentito il Comitato di applicazione del Codice di autoregolamentazione media e minori, «promuove forme di co-regolamentazione e di autoregolamentazione tramite codici di condotta, nel rispetto di quanto previsto dagli articoli 4-bis e 28-ter della direttiva 2010/13/UE del Parlamento europeo e del Consiglio del 10 marzo 2010, come da ultimo modificata dalla direttiva 2018/1808/UE del Parlamento europeo e del Consiglio del 14 novembre 2018»; Parere del Comitato economico e sociale europeo sul tema "Autoregolamentazione e co-regolamentazione nel quadro legislativo dell'UE" del 4 settembre 2015, in che definisce la regolamentazione come "forma di regolamentazione delle parti interessate (stakeholder) che è promossa, orientata, guidata o controllata da una terza parte (sia essa organismo ufficiale o un'autorità di regolamentazione indipendente) di norma dotata di poteri di esame, di controllo e, in alcuni casi, sanzionatori" (punto 3.4).

anche in mancanza di un simile recepimento da parte del legislatore, le norme deontologiche assumono valore giuridico nella misura in cui, attraverso la puntualizzazione di specifici doveri comportamentali, esplicano principi generali di correttezza e diligenza (Bellelli, 2014; Valongo, 2014), facendo così sorgere situazioni giuridiche soggettive meritevoli di tutela nei confronti dei terzi. In virtù del principio di sussidiarietà orizzontale (art. 118, ult.c., Cost.) che fa retrocedere la legge di fronte a fenomeni di regolamentazione provenienti dal basso, tali norme non sono semplici regole morali o autonome, interne alla categoria professionale, ma sono regole giuridiche, complementari rispetto alla legislazione statale.

In coerenza con tale impostazione, il *Codice di autoregolamentazione Internet e minori* non si limita ad impegnare le piattaforme che liberamente vi aderiscono, ma ha un valore vincolante per qualsiasi soggetto operante *online*, anche per chi non abbia ad esso espressamente aderito e a prescindere dal tipo di infrastruttura di rete. A riprova della intrinseca forza normativa di tale Codice di condotta, la disposizione di cui al comma 6 dell'art. 37 del TUSMA prevede che «I fornitori di servizi di media diffusi tramite qualsiasi canale o piattaforma sono obbligati ad osservare le disposizioni a tutela dei minori previste dal *Codice di autoregolamentazione media e minori*. Il Codice e l'adozione di eventuali nuovi atti di autoregolamentazione sono recepiti con decreto del Ministro dello sviluppo economico, adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, previo parere della Commissione parlamentare di cui alla legge 23 dicembre 1997, n. 451 e successive modificazioni»³.

Nell'ultimo ventennio, unitamente allo sviluppo della *soft law* nel mondo dell'economia digitale, una profonda evoluzione ha riguardato la società dell'informazione e dell'informatica sul piano della produzione normativa. Dopo l'emanazione del d.lgs. 9 aprile 2003 n. 70, di attuazione della direttiva 2000/31/CE sul commercio elettronico, la rete telematica mondiale (*www*, acronimo di *world wide web*) è divenuta potenzialmente accessibile a tutti non solo tramite un *computer*, ma anche mediante dispositivi elettronici innovativi (*tablet*, *smart-phone*, *smart-tv*, *smart-watch*, etc.), che diffondono servizi digitali sempre più complessi con l'insorgenza di pericoli in passato sconosciuti. Da quel momento,

³ In attuazione dell'art. 3 della legge 22 aprile 2021, n. 53, recante «Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - legge di delegazione europea 2019-2020», con l'atto n. 109 il Governo italiano sottopone al parere del Parlamento un testo di correzioni al d.lgs. n. 208 del 2021, (c.d. TUSMA). In particolare, si vuole sostituire il comma 6 dell'art. 37 con il seguente: «6. I fornitori di servizi di media diffusi tramite qualsiasi canale o piattaforma sono obbligati a dotarsi di un Codice di autoregolamentazione a tutela dei minori. Il Codice e l'adozione di eventuali nuovi atti di autoregolamentazione su parere del comitato consultivo di cui all'articolo 8 sono recepiti con decreto del Ministro delle imprese e del made in Italy, adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, previo parere della Commissione parlamentare di cui alla legge 23 dicembre 1997, n. 451».

prevale l'idea che il legislatore italo-europeo non possa lasciare la dimensione del web esclusivamente al diritto mite.

Più che semplice luogo di socializzazione (*social media*), *Internet* è oggi una piazza ideale, una *e-agerà*, nella quale ogni attività della vita quotidiana di tipo tradizionale viene svolta con modalità a distanza. Le piattaforme digitali hanno perso la loro funzione di meri fornitori di connessione alla rete per diventare non solo «offerenti» di beni e servizi, protagonisti di qualsiasi genere di transazione commerciale, operanti in concorrenza con imprese spesso non dotate di tale potenzialità, ma anche «intermediari», ossia soggetti che fanno incontrare domanda e offerta, rendendo possibili relazioni di scambio sia fra imprese e consumatori (*business to consumer*, B2C), sia fra gli stessi imprenditori (*business to business*, B2B). Le infrastrutture di rete creano nei confronti di tutti gli utenti - commerciali e non - una forte dipendenza, soprattutto perchè capaci, mediante l'impiego di algoritmi (sistemi di Intelligenza Artificiale), di controllare i flussi delle informazioni circolanti a livello globale, di catalogare enormi quantità di dati (*big data*), di ordinarli, selezionarli, classificarli in schemi e, quindi, di manipolarli discrezionalmente. Si avverte pertanto la necessità di applicare a tutti gli utenti che instaurino con esse rapporti negoziali le disposizioni a tutela del consumatore, al fine di superare l'asimmetria di potere che connota questi rapporti (Mezzasoma, Rizzo, Ricciuto e Llamas Pombo, 2016; Perlingieri, G., Mezzasoma e Angelone, 2024).

Le piattaforme *online*, esercitando il loro potere «sovrano», incidono in vario modo sui diritti delle persone e acquisiscono intere porzioni di mercato. L'organizzazione dei *big data* in base alla tipologia di utente permette loro di predire i comportamenti e di raccogliere sempre più dati personali che diventano un patrimonio aziendale fondamentale sul quale si basano le attività di marketing. I dati che interessano maggiormente a fini commerciali sono le preferenze di coloro che usufruiscono dei servizi, mediante le quali è possibile tracciare il «profilo» degli utenti.

Il carattere innovativo dei servizi digitali risiede, dunque, nella circostanza che la piattaforma non riveste una posizione di neutralità ovvero di mera ospitalità di pagine web rese accessibili al pubblico, ma è in grado di gestire i dati immessi nella piattaforma e, pertanto, svolge una funzione attiva, potendo promuovere gli scambi, suggerire determinati contenuti o raccomandare determinate scelte⁴. Attualmente le piattaforme, nell'esercizio del

⁴ Attraverso i c.d. *cookies*, le piattaforme raccolgono informazioni relative all'utente; si dedicano alla ricerca, alla «profilazione» e al monitoraggio dei potenziali acquirenti. Tutto ciò al fine di inviare a determinate categorie di utenti messaggi pubblicitari in linea con le preferenze manifestate nel corso della navigazione in rete (c.d. pubblicità mirata).

loro “potere sovrano”, sono nel contempo decisori, controllori e regolatori della contrattazione, perchè dettano le regole del gioco, scelgono quali contenuti inserire nel sito e decidono persino la sospensione di un *account*, grazie all’utilizzo di mezzi automatizzati di valutazione dell’operato umano.

L’attuale evoluzione della Società dell’Informazione nella Società dell’Algoritmo, ossia in un nuovo modello sociale governato dall’automazione e connotato dallo sviluppo di nuovi prodotti e servizi potenzialmente invasivi della vita di ogni persona, ha reso insufficiente la sola auto-regolamentazione proveniente dal “basso” e necessaria l’emanazione di norme eteronome, di matrice pubblicistica.

Nel contesto descritto, i minori vedono accrescere le possibilità di esprimersi e di avere l’accesso ad una quantità infinita di informazioni, nonchè di appropriarsi di beni e servizi di ogni genere offerti dagli *Internet Service Providers* (Perlingieri C., 2014; Giova, 2014; Gambino, 2015; Perlingieri P., 2018; Di Sabato, 2020). Una prima conseguenza negativa di tale fenomeno risiede nel fatto che, in cambio di un bene o servizio, i minori autorizzano le piattaforme *online* al trattamento dei propri dati personali, che vengono sfruttati economicamente tramite l’impiego di Intelligenza Artificiale, senza che essi ne abbiano consapevolezza.

L’impatto che la rinnovata *platform economy* ha prodotto sul mondo dell’infanzia e dell’adolescenza ha indotto le istituzioni europee e nazionali ad intervenire per rafforzare l’assetto normativo della protezione.

Nel panorama attuale, regolamentazione pubblica e privata si integrano a vicenda e la co-regolazione diventa il caposaldo del nuovo impianto normativo di salvaguardia dei minori dai rischi della rete.

2 L’INSUFFICIENZA DEL CONSENSO INFORMATO COME STRUMENTO DI PROTEZIONE NELLA SOCIETÀ DELL’ALGORITMO

Questa tendenza è agevolata dai c.d. effetti di rete (*network effects*), che consistono nell’innalzamento del valore dei beni o servizi prodotti online con l’aumento del numero degli utenti. Questi effetti sono in grado di incidere negativamente sia sul versante concorrenziale, incrementando le posizioni dominanti delle imprese, sia sul versante consumeristico, in quanto scoraggiano gli utenti dal passaggio da una piattaforma all’altra per ottenere un servizio equivalente, con evidente restrizione del libero mercato: la scelta di cambiare fornitore, infatti, determinerebbe ulteriori costi e anche la perdita di dati personali forniti come corrispettivo per la fruizione del servizio. In giurisprudenza, v. Consiglio di Stato, 29 marzo 2021, n. 2631 (in *Nuova giurisprudenza civile commentata*, 2021, 5, p. 1079), il quale parla di «patrimonializzazione del dato personale» attuata attraverso la messa a disposizione del dato ad opera di un social network a fini commerciali e soprattutto attraverso la profilazione dell’utente; ciò rende applicabile la tutela consumeristica per garantire una "protezione multilivello" dei diritti delle persone fisiche che deve realizzarsi quando un diritto personalissimo sia sfruttato a fini commerciali.

Per offrire ai minori una minima protezione *online*, l'Unione Europea ha sancito una regola generale relativa al consenso alla fruizione dei relativi servizi: l'art. 8 del Regolamento UE sulla Protezione dei Dati Personali n. 679 del 27 aprile 2016 (*General Data Protection Regulation*, GDPR) vieta l'offerta di servizi digitali a coloro che non hanno compiuto 16 anni, a meno che non sia raccolto il consenso dei genitori. Lo stesso art. 8 del GDPR stabilisce che gli Stati membri possono stabilire per legge un'età minima inferiore, purchè superiore ai 13 anni. Il legislatore italiano, adeguandosi al GDPR mediante il d.lgs. 10 agosto 2018 n. 101, ha sancito un abbassamento a 14 anni del limite di età per esprimere il consenso al trattamento dei dati personali del minore nell'ambito dei servizi elettronici. In tal senso, l'art. 2 *quinquies*, del d.lgs. 2003 n. 196 (*Codice della privacy*) introduce una deroga di ampia portata alla regola di cui all'art. 2 c.c. secondo la quale la capacità di agire si acquista al compimento dei 18 anni (Stanzione, 1980; Giardina, 1984; Rescigno, 1988; Bocchini, 2000). In tal modo è stata introdotta una sorta di "maggiore età digitale" alla soglia dei 14 anni, che delinea un diritto fondamentale dell'ultraquattordicenne non solo di accedere alla rete senza il consenso dei genitori, ma anche di manifestare liberamente il proprio pensiero a mezzo Internet e di interagire con il mondo virtuale, in attuazione degli art. 21 e art. 13 della Costituzione italiana e dell'art. 13 della Convenzione ONU sui diritti dell'infanzia e dell'adolescenza.

Il Considerando n. 38 del GDPR specifica, altresì, che il consenso dei genitori non è necessario per utilizzare i servizi di prevenzione o i servizi di consulenza forniti direttamente ai minori, che hanno come finalità quella di proteggere i minori da fatti illeciti provenienti da terzi.

La strategia introdotta dall'art. 8 del GDPR rappresenta solo un primo passo per contrastare i pericoli che i minori incontrano in rete per le ragioni di seguito esposte.

In primo luogo, numerose sono le difficoltà che le piattaforme *online* incontrano nell'acquisizione e nell'accertamento del consenso dei genitori, ove necessario. Ai sensi dell'art. 8, par. 2, del GDPR, infatti, il fornitore di servizi *online* deve adoperarsi per verificare che il consenso del titolare della responsabilità genitoriale sia effettivamente prestato "in considerazione delle tecnologie disponibili", ma queste "tecnologie disponibili" sono sistemi, talvolta complicati, che possono essere sempre aggirati dal minore, il quale potrebbe far apparire come presente un'autorizzazione genitoriale in realtà inesistente.

Sembra che il GDPR non tenga nella dovuta considerazione i trattamenti effettuati nei confronti della globalità degli utenti e che si riferisca essenzialmente allo scambio individuale

di dati, dall'interessato al titolare del trattamento, subordinato al consenso dell'interessato; anche gli eventuali successivi trasferimenti di dati restano subordinati al consenso. Tuttavia, rispetto al momento in cui fu emanato il GDPR, la tecnologia è, come già posto in luce, notevolmente mutata e ora emerge l'insufficienza della regola del consenso informato come unico ed esclusivo strumento di tutela del minore *online*.

Il perfezionamento di dispositivi *smart* e la crescente diffusione dei *social network* e dei motori di ricerca hanno fatto sì che oggi le informazioni siano destinate fin dall'origine alla condivisione da parte di un numero indefinito di persone, alla circolazione su larga scala e alla cogestione a livello globale (Perlingieri, P. 2018; Fachechi, 2023). Pertanto, la normativa del GDPR, centrata sul controllo "individuale" dei dati, non riesce da sola a garantire una tutela efficace nella realtà attuale, ove si tratta di proteggere i dati di masse di persone (*big data*), specie di persone vulnerabili come i minori.

Il «consenso informato» della persona - minore ultraquattordicenne o dei genitori - al trattamento dei dati personali, per l'accesso alla piattaforma digitale, non rappresenta un mezzo adeguato di protezione, in primo luogo, perché non è mai veramente «informato», attesa la difficoltà di comprendere la complessità dei termini e delle informazioni presenti nelle condizioni generali dei servizi (che gli utenti non sono soliti leggere); in secondo luogo, perché esso è richiesto come condizione indispensabile per usufruire del bene o servizio, il che implica che la scelta dell'utente non è mai libera, ma sempre necessitata dal bisogno di ottenere quel bene o servizio.

Anche la fissazione del limite d'età per l'accesso alla rete non si rivela misura adatta a tutelare il minore (Perlingieri C., 2016), non solo in quanto facilmente aggirabile, ma anche perché la regola sul consenso al trattamento digitale (art. 8, GDPR) male si coordina con le regole relative alla validità e all'efficacia dell'atto posto in essere dal minore (artt. 1425 e 1426 c.c.). Mentre, sul piano giuridico, consenso al trattamento dei dati personali e consenso alla conclusione del contratto si distinguono, nella realtà pratica, invece, tendono a sovrapporsi, in quanto il piano patrimoniale interagisce con il piano personale, dal momento che i dati personali presentano una duplice anima, trattandosi di interessi di natura esistenziale che sono parimenti oggetto di valutazione economica.

Quando si tratta di compiere scelte personalissime che hanno ricadute sul piano patrimoniale, si dovrebbe prescindere da limiti di età fissati in astratto e far leva sulla sussistenza della «capacità di discernimento», intesa come abilità a comprendere il valore di singole decisioni, a valutarne i rischi e i benefici, sempre con riferimento al caso concreto.

Nel momento in cui i minori acquistano in rete beni o servizi, realizzano un'attività consueta della vita, che non potrebbe essere loro negata, altrimenti ne deriverebbe un ostacolo all'esercizio dei loro diritti e libertà fondamentali. La tesi trova corrispondenza nella posizione assunta dalla dottrina prevalente (Dosi, 1995; Bianca, 2002; Senigaglia, 2022), secondo il quale i minori possono stipulare i contratti necessari a soddisfare normali esigenze della quotidianità, purchè capaci di discernimento e purchè quegli atti non li esponano ad un rilevante pregiudizio. Coerentemente con tale visione, i minori, oltre ad avere una capacità giuridica per averla acquisita al momento della nascita (art. 1, comma 1, c.c.), sono reputati titolari di una «capacità di agire anticipata» nella sfera esistenziale. Tale capacità li rende *a priori* idonei a compiere anche in campo patrimoniale atti strumentali allo sviluppo della personalità (c.d. contratti identitari della vita corrente) purchè di scarso peso economico (Berti De Marinis, 2016). Pertanto gli acquisti *online* di esiguo valore dovrebbero ritenersi validi ed efficaci, se il minore - anche infraquattordicenne - abbia acquisito una capacità di discernimento; si pensi alle ipotesi in cui un dodicenne «scarica» a pagamento un *compact disc* musicale.

In questa prospettiva, sembra doversi riconoscere al minore - indipendentemente dal raggiungimento dei quattordici anni ma sempre sul presupposto dell'assenza di un pregiudizio rilevante - una capacità negoziale di “cedere” i propri dati personali in corrispettivo della fornitura di contenuti o servizi digitali, operazione regolata in generale dal d.lgs. 2021 n. 173 (di attuazione della direttiva del 2019 n. 770).

3 INTERVENTI SOSTANZIALI DEL LEGISLATORE ITALIANO IN TEMA DI CYBERBULLISMO

I servizi digitali vengono spesso prestati in modo abusivo dalle piattaforme *online* che, anche mediante l'impiego dell'Intelligenza artificiale, ledono diritti fondamentali del minore: non solo diritti individuali (al nome, all'immagine, all'onore, alla reputazione, alla privacy, allo sviluppo e alla promozione della personalità), ma anche diritti sociali, quali il diritto alla salute, all'ambiente, al lavoro.

Come accennato, i contenuti illegali trasmessi in rete possono sfuggire al controllo dei genitori quando i minori creano profili *fake* ed entrano in contatto con utenti sconosciuti in grado di approfittare della loro condizione, attraverso l'utilizzo di *user id* o *avatar* falsi. Si assiste all'uso improprio delle piattaforme *online*, che esponono i soggetti in età evolutiva a

fatti gravemente dannosi, quali la manipolazione o sottrazione di dati, la dispersione di notizie ingannevoli e di altri contenuti illeciti, l'incitamento al bullismo, l'*hate speech* (linguaggio di odio razziale, sessuale, religioso o etnico), il *revenge porn* (diffusione di materiale intimo), il *grooming* (adescamento *online*), l'offerta di materiale pornografico e di altri beni o servizi pericolosi, il *social washing* (come il più noto *greenwashing*), che si verifica quando un'affermazione di sostenibilità contiene informazioni false circa il rispetto di valori, come la salute, la sicurezza dei prodotti, la privacy dei dati, la tutela dell'ambiente.

Dinanzi a tale scenario si avverte l'esigenza di passare da un'ottica formalistica, basata essenzialmente sull'informazione e sul consenso, ad un'ottica sostanzialistica, che si fonda su una politica di controllo dei contenuti immessi e diffusi in rete, al fine di evitare e soprattutto prevenire la causazione di danni. In tal senso si è mosso il legislatore nazionale con particolare riferimento alla prevenzione ed al contrasto del fenomeno del cyber bullismo (Citarella, 2023). La legge 29 maggio 2017 n. 71 ha previsto al riguardo una procedura stragiudiziale di *notice and take down* (analoga a quella già prevista dall'art. 21, c. 2, direttiva 2000 n. 31) attivabile in via di urgenza anche dall'ultraquattordicenne - e perfino all'insaputa dei genitori - di fronte ad atti di «cyberbullismo», che si identificano con «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» (art. 1, comma 2).

La legge 2017 n. 71 dispone che ciascun minore con più di 14 anni, anche senza il consenso del genitore, oppure il genitore, possono inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco di qualsiasi contenuto lesivo nei confronti del minore, individuato dallo stesso danneggiato tramite l'indirizzo URL (*Uniform Resource Locator*) che identifica ogni sito web. L'intervento dei genitori diviene necessario solo in un secondo momento e soltanto in caso di mancata osservanza della richiesta, cioè se entro 24 ore il gestore non abbia provveduto a comunicare di essersi attivato per conformarsi all'istanza ovvero se entro 48 ore non abbia provveduto direttamente all'oscuramento o al blocco del contenuto illecito. In questo secondo caso, è prevista la possibilità di ricorrere alla Autorità Garante per la

protezione dei dati personali, che dovrà disporre la rimozione o il blocco del contenuto entro le successive 48 ore, ai sensi degli artt. 143 e 144 del d.lgs. 2003 n. 196.

Inoltre la stessa legge cyberbullismo ha introdotto misure educative con finalità social-preventiva in ambito familiare e in ambito scolastico, incentivando soprattutto la formazione dei genitori e del personale docente e non (artt. 3, 4 e 5, l. 2017 n. 71). Le istituzioni scolastiche devono promuovere l'educazione all'uso consapevole della rete internet e ai diritti e doveri ad esso connessi. In ambito extrascolastico, si prevede che i servizi sociali, anche con l'aiuto delle associazioni, promuovano progetti personalizzati per sostenere non solo le vittime di cyber bullismo, ma anche per rieducare i minori autori di cyber bullismo mediante attività riparatorie o di utilità sociale.

Sempre verso una direzione di protezione sostanziale, si sono rivolte le istituzioni europee nell'ultimo ventennio, consapevoli della necessità di intervenire in via anticipata per evitare pregiudizi ai minori e specialmente per impedire che si ripropongano in futuro.

4 IL *DIGITAL SERVICE ACT* E IL PROBLEMA DELLA PROTEZIONE DEI MINORI DAGLI ABUSI SESSUALI *ONLINE*

Dinanzi alle criticità, in precedenza evidenziate, dell'applicazione della regola del consenso al controllo dei *big data*, il *Digital Service Act* (Regolamento UE del 19 ottobre 2022 n. 2065) detta norme volte alla supervisione delle attività *ex ante* secondo una strategia risk-based, allo scopo di garantire una protezione efficace alle masse di persone, superando la logica della mera gestione individuale dei dati.

L'obiettivo del *Digital Service Act* è creare uno spazio digitale più sicuro, prevedibile e affidabile, non solo all'interno del mercato unico europeo, ma, tendenzialmente, a livello transnazionale: infatti, si applica a tutti gli intermediari che offrono servizi nell'Unione Europea o hanno un collegamento sostanziale con l'Unione, indipendentemente dalla circostanza che la loro sede sia localizzata all'interno dell'UE.

L' Art. 28 (*Protezione online dei minori*) del *Digital Service Act* stabilisce che i fornitori di piattaforme *online* accessibili ai minori sono tenuti ad adottare «misure adeguate e proporzionate» per evitare danni ai minori; ad esempio, progettando le loro interfacce *online* in modo da garantire il massimo livello di privacy, sicurezza e protezione dei minori per impostazione predefinita, adottando norme o aderendo a codici di condotta per la protezione

dei minori. Ad esempio, alcune condizioni generali di accesso ai servizi, predisposte dai fornitori, non accettano l'iscrizione dei minori di anni 14. Altre piattaforme *online* (es. *Vinted*, *E-bay*,) inseriscono tra i termini e le condizioni la disposizione secondo la quale le persone che intendono registrarsi ai siti o acquistare prodotti devono possedere la maggiore età al momento della registrazione o della conclusione del contratto. Qualche piattaforma, però, è congegnata in modo tale che soltanto nell'ultima fase di accesso, ossia dopo aver avviato la registrazione dell'account e confermato l'operazione tramite e-mail, l'utente scopre che si tratta di un servizio "vietato ai minori", il che favorisce la creazione di profili *fake* e la conseguente diffusione di dati non veritieri⁵. Problemi si pongono non solo quando l'utente trasmette dati identificativi falsi, ma anche quando uno stesso dispositivo elettronico viene utilizzato da più persone, maggiorenni e minorenni.

Il citato art. 28 del *Digital Service Act*, nel secondo paragrafo, vieta ai fornitori *online* di proporre sull'interfaccia messaggi pubblicitari basati sulla profilazione del destinatario del servizio se sono consapevoli, «con ragionevole certezza», che il destinatario del servizio è un minore. Come può, tuttavia, la piattaforma essere «ragionevolmente certa» che il destinatario del servizio sia un minore? Ancora una volta, il problema è di assicurare una procedura di verifica dell'età dell'utente. Tale aspetto sarà ripreso nell'ultimo paragrafo del presente lavoro.

Rispetto alle norme, facilmente eludibili, che precludono l'ingresso alla rete in base all'età, più efficaci risultano le regole che escludono *ab origine* l'immissione nel web di contenuti inappropriati per i minori, anche se il quadro europeo al riguardo non pare pienamente soddisfacente.

Di segno positivo sono sicuramente le disposizioni del *Digital Services Act* che reputano l'adesione a un determinato codice di condotta, e il suo rispetto da parte di una piattaforma *online*, quali misure di attenuazione dei rischi adeguate per impedire attività dannose per i minori, come la manipolazione dei *big data*, l'utilizzo di *account* falsi o di *bot* (cioè risposte automatiche, i c.d. *like*) non veritieri (v. Considerando 104). In particolare, in base al *Digital Service Act*, la circostanza che un fornitore *online* rifiuti l'invito della Commissione europea a partecipare all'applicazione di un codice di condotta può essere presa in considerazione nel determinare se siano stati violati gli obblighi imposti normativamente.

⁵ Se il minore dichiara un'età falsa, la piattaforma dovrebbe cercare di risalire all'età della persona e, ove risulti che quella persona non ha 14 anni, dovrebbe comunicare - tramite e-mail - ai genitori l'iscrizione alla piattaforma illegittimamente effettuata dal figlio, così da permettere agli esercenti la responsabilità genitoriale di intervenire a salvaguardia del minore.

Occorre, peraltro, evidenziare che la mera partecipazione all'elaborazione di un determinato codice di condotta non presuppone, di per sé, la conformità al regolamento stesso.

Alcune perplessità sollevano le previsioni del *Digital Service Act*, secondo le quali i prestatori di servizi di intermediazione *online* possono avviare di propria iniziativa indagini volontarie e attività di «moderazione dei contenuti» (art. 3, lett. t, *Digital Service Act*) per «individuare, identificare e contrastare contenuti illegali e informazioni incompatibili con le condizioni generali» e devono agire immediatamente per rimuoverli non appena ne vengano effettivamente a conoscenza, adottando anche misure quali «la cessazione o la sospensione dell'account di un destinatario del servizio» e fornendo sempre una motivazione chiara e specifica delle restrizioni imposte. In altri termini, le *big tech*, tramite i loro apparati para-giurisdizionali e para-sanzionatori, hanno la possibilità di eliminare contenuti illeciti segnalati da terzi, di disabilitare l'accesso a quei contenuti, di sospendere le attività dell'utente che li abbia pubblicati e finanche di chiudere l'*account* di tale utente.

Entro i limiti suddetti, ai gestori delle piattaforme viene attribuito un potere di controllare la liceità dei contenuti inseriti nella rete, che potrebbero nuocere alla salute o allo sviluppo fisico e mentale dei minori. Si avverte pertanto la necessità di sviluppare sistemi (anche algoritmici) sempre più perfezionati, in grado di oscurare contenuti lesivi della persona del minore, a prescindere dall'età dichiarata dal titolare del relativo *account* e di giungere, ove necessario, anche alla disattivazione del profilo.

Resta, tuttavia, critico il fatto che il Regolamento UE 2022 n. 2065 si limiti a porre la regola non della responsabilità, ma della «responsabilizzazione» dei prestatori di servizi digitali, il che implica che questi ultimi rispondano per i contenuti illegali pubblicati tramite le loro piattaforme soltanto nel caso in cui, una volta venuti a conoscenza dell'illecito, non abbiano agito tempestivamente per rimuoverne il contenuto⁶ (art. 5, lett. e, *Digital Service Act*); di conseguenza, restano esentati da responsabilità ove ignari di tali contenuti, non avendo un obbligo generale di sorveglianza di quanto postato in Internet (artt. 14-17, d.lgs. 2003 n. 70).

Non convince neppure il disposto del *Digital Services Act*, che confina l'esercizio dei suddetti poteri-doveri all'ipotesi in cui l'*Internet Service Provider* ritenga fondata la

⁶ In questa direzione, in giurisprudenza, si vedano: Corte di Cassazione, 19 marzo 2019, n. 7708 (in *Giurisprudenza italiana*, 2019, p. 2604), la quale non esclude la responsabilità del *provider* che fornisca servizi di *hosting* attivo, cioè servizi che comportano il suo coinvolgimento nella gestione delle informazioni; Corte di Cassazione, ordinanza 8 giugno 2022, n. 18430 (in *Danno e responsabilità*, 2022, 6, p. 724), secondo la quale il prestatore del servizio di *hosting* è responsabile con riguardo al contenuto delle informazioni ai sensi dell'art. 16 del d.lgs. n. 70 del 2003, quando egli sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione, oppure egli non agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso appena avuta conoscenza di tali fatti, su comunicazione delle autorità competenti.

segnalazione di illegalità proveniente da terzi. In tal modo, infatti, la garanzia della conformità all'ordinamento giuridico è rimessa alla determinazione degli stessi *Providers*. La discrezionalità di questi ultimi sussiste non solo nel valutare l'effettiva illegalità del contenuto, ma anche nell'individuare il «giusto rimedio», ossia nel decidere se il provvedimento più adeguato sia quello di mera rimozione del contenuto o di sospensione provvisoria della fornitura del servizio o, addirittura, quello di disabilitazione dell'*account* di chi lo ha inserito nel web. Tale intervento di moderazione sembrerebbe atteggiarsi come un ordine inibitorio impartito da un giudice, adottabile anche in via preventiva, ma non si tratta di un procedimento giudiziario, bensì di uno strumento interno di auto-controllo che ha carattere privato e che il *provider* attiva solo dopo l'immissione in rete; non appare, perciò, sufficiente sul piano rimediale, perché la salvaguardia dei diritti lesi è rimessa alla volontà del gestore delle piattaforme e soprattutto perché è pur sempre un intervento successivo alla commissione dell'illecito. A dimostrazione di quanto osservato, si richiama la norma secondo la quale i destinatari del servizio possono contestare le decisioni delle piattaforme *online* relative all'illegalità di contenuti, attraverso un reclamo volto all'annullamento delle decisioni contestate; il reclamo deve essere disponibile per almeno sei mesi, da calcolarsi a partire dal momento in cui la piattaforma ha informato il destinatario del servizio della decisione (art. 20, *Digital Service Act*). Tale meccanismo è regolato in modo tale che i provvedimenti di moderazione dei contenuti vengano comunicati solo dopo che siano stati già pubblicati, al fine di permettere di proporre entro sei mesi un eventuale reclamo presso il *Coordinatore dei servizi digitali* dello Stato membro in cui il destinatario del servizio è situato.

In definitiva, il sistema di segnalazione volontaria così congegnato non risulta efficace, perché, lungi dall'evitare *ex ante* l'inserimento in rete di contenuti lesivi, consente che il fatto illecito perpetrato nei confronti dei minori continui, almeno per un certo lasso di tempo, a produrre danni.

La scarsa efficacia sul piano rimediale si nota specialmente con riferimento alla rilevazione e alla rimozione degli abusi di carattere sessuale. A livello europeo, si osserva che le misure intraprese contro l'adescamento di minori e la diffusione di materiale pedopornografico sono assai diverse le une dalle altre e che le segnalazioni provengono soltanto da singoli gruppi di prestatori di servizi *online*, mentre tutti gli *Internet providers* dovrebbero svolgere un ruolo primario nell'allertare e favorire l'intervento immediato delle autorità di pubblica sicurezza. Per questa ragione, l'11 maggio 2022, il Parlamento europeo ha adottato una *Proposta di Regolamento UE per la prevenzione e la lotta contro l'abuso*

sessuale su minori, che pone obblighi giuridici a carico dei prestatori di servizi *online* di rilevare l'abuso sessuale sui minori, di segnalarlo in via d'urgenza alle autorità di polizia e di rimuovere il materiale pedopornografico⁷. A questi fini, nella *Proposta di Regolamento* si prevede l'istituzione di un Centro dell'UE, che dovrà cooperare con le autorità nazionali di ciascuno Stato membro e assisterle nella fase di attuazione del Regolamento. Il Centro, in particolare, dovrà gestire apposite banche dati - predisposte in ogni Paese e finanziate dalla Commissione europea - mediante le quali i gestori delle piattaforme dovranno ottemperare ai loro obblighi a sostegno delle vittime.

E' fortemente auspicabile l'approvazione di tale *Proposta di Regolamento*, dal momento che le strategie in essa prefigurate sembrano in grado di proteggere i minori in modo più adeguato rispetto a quanto previsto nel *Digital Services Act*, sia pure limitatamente a fatti di particolare gravità.

5 IL SISTEMA ITALIANO DI ETICHETTATURA DEI CONTENUTI DANNOSI A TUTELA DELLE PERSONE VULNERABILI: IL *TESTO UNICO DEI SERVIZI DI MEDIA AUDIOVISIVI*

Una disciplina più pregnante sotto il profilo della difesa dei diritti dei minori *online* è contenuta nel d.lgs. 8 novembre 2021 n. 208 (TUSMA), che, abrogando il d.lgs. n. 177 del 2005 (c.d. legge Gasparri) e dando attuazione alla Direttiva europea n. 1808 del 14 novembre 2018, prevede un congegno articolato di disposizioni normative rivolte alle piattaforme soggette alla giurisdizione italiana e dirette a garantire la trasmissione dei servizi di media che rispettino i diritti fondamentali della persona e a salvaguardare tutti i minori mediante «rigorose misure di controllo dell'accesso» ai contenuti maggiormente nocivi (art. 42, comma 6, TUSMA).

Il TUSMA detta i seguenti principi generali per la prestazione di servizi di media digitali a garanzia degli utenti: «a) libertà e pluralismo dei mezzi di comunicazione radiotelevisiva; b) libertà di espressione di ogni individuo, inclusa la libertà di opinione e quella di ricevere o di comunicare informazioni o idee senza limiti di frontiere, nel rispetto della dignità umana, del principio di non discriminazione e di contrasto ai discorsi d'odio; c)

⁷ La *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l'abuso sessuale su minori* (Bruxelles, 11.5.2022 - COM(2022)) è consultabile nel sito: <https://eur-lex.europa.eu>.

obiettività, completezza, lealtà e imparzialità dell'informazione; d) contrasto alle strategie di disinformazione; e) tutela dei diritti d'autore e di proprietà intellettuale; f) apertura alle diverse opinioni e tendenze politiche, sociali, culturali e religiose; g) salvaguardia delle diversità etniche e del patrimonio culturale, artistico e ambientale, in ambito nazionale e locale, nel rispetto delle libertà e dei diritti, in particolare della dignità della persona e della protezione dei dati personali, della promozione e tutela del benessere, della salute e dell'armonico sviluppo fisico, psichico e morale del minore, garantiti dalla Costituzione, dal diritto dell'Unione europea, dalle norme internazionali vigenti nell'ordinamento italiano e dalle leggi statali e regionali; h) contrasto alla tendenza contemporanea di distruggere o comunque ridimensionare gli elementi o simboli della storia e della tradizione della Nazione (cancel culture).»

La novità più incisiva risiede nell'estensione ai servizi di media c.d. non lineari (piattaforme digitali per la condivisione di video, *social network*, servizi audiovisivi *on demand*) dei divieti già precedentemente disposti a protezione dei minori per i servizi di media c.d. lineari, diffusi per lo più tramite supporti televisivi. La portata del TUSMA è così ampia da includere tutti i servizi di accesso a qualsiasi piattaforma di diffusione, indipendentemente dalla tecnologia di trasmissione.

In tal modo, l'Italia, differenziandosi da altri Stati europei, prevede un meccanismo vincolante di *rating*, imponendo una classificazione di fasce orarie di programmazione, da sottoporre a revisione periodica: i programmi rivolti ai minori o potenzialmente nocivi per i minori, devono essere classificati dalle stesse piattaforme mediante un sistema di etichettatura chiaramente evidente, che consenta agli utenti di riconoscere il livello di adeguatezza per i minori. Tale classificazione deve avvenire nel rispetto di determinati criteri che vengono fissati dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM, istituita dall'art. 1, comma 4, del d.lgs. 31 luglio 1997, n. 249) con apposite «procedure di co-regolamentazione», con la conseguenza che i Regolamenti emanati dall'AGCOM diventano fondamentali per garantire una navigazione sicura ai minori, potendo individuare persino misure tecniche aggiuntive rispetto a quelle previste dal TUSMA. L'AGCOM è poi chiamata successivamente a vagliare se l'etichettatura sia stata predisposta correttamente dalla piattaforma ed eventualmente ad imporre sanzioni.

Appare, dunque, evidente, che il TUSMA accresce le tutele, perchè stabilisce orari del giorno e della notte, durante i quali determinati contenuti non possono essere trasmessi, a prescindere dall'età dei possibili destinatari dei servizi media e, dunque, a protezione di tutte

le persone vulnerabili⁸. Al comma 9 dell'art. 37 del TUSMA è previsto che i dati personali relativi a minori comunque raccolti dai fornitori «non possono essere trattati a fini commerciali e, in particolare, a fini di marketing diretto, profilazione e pubblicità mirata sulla base dei comportamenti rilevati». E' vietata qualsiasi pubblicità che induca il minore a persuadere i genitori ad acquistare prodotti o servizi ed è vietata la pubblicità che mostri i minori in situazioni pericolose.

L'art. 42 del TUSMA definisce, inoltre, le *Misure di tutela* che i fornitori di piattaforme *online* devono adottare.

Tra gli obblighi imposti ai fornitori di servizi dall'art. 42 del TUSMA si segnalano: l'obbligo di predisporre meccanismi di facile uso che consentano agli utenti di valutare i contenuti e di segnalare alle stesse piattaforme i dati illegali immessi in rete; l'obbligo di dotarsi di sistemi di controllo parentale e l'obbligo di utilizzare, nel rispetto della normativa in materia di protezione dei dati personali, sistemi di verifica dell'età degli utenti in modo da evitare che determinati contenuti possano nuocere ai minori; l'obbligo di predisporre procedure trasparenti, di facile uso ed efficaci per la gestione e la risoluzione dei reclami degli utenti; l'obbligo di predisporre misure e strumenti efficaci di alfabetizzazione mediatica e sensibilizzare gli utenti in merito a tali misure.

Nell'ambito di tale complesso strumentario di tutele, l'AGCOM assume un ruolo centrale, in primo luogo come ente di normazione, in gran parte rimessa alle sue Linee guida, che vengono adottate con la partecipazione dei soggetti interessati. A tal fine sono, infatti, chiamati ad esprimere il loro parere: l'Autorità garante per l'infanzia e l'adolescenza, il Comitato di applicazione del *Codice di autoregolamentazione media e minori* e le stesse piattaforme online. Queste ultime cooperano alla definizione dei regolamenti dell'AGCOM (art. 37, comma 1) che presuppongono la consultazione pubblica di associazioni di categoria del settore delle comunicazioni, di associazioni dei consumatori, delle imprese telefoniche, il che rende l'*Authority* più vicina alle persone, dialogando con gli operatori del settore. Tale

⁸ Ai sensi del comma 7 dell'art. 37 del d.lgs. 2021 n.208, i fornitori di servizi di media sono obbligati ad applicare, anche secondo quanto stabilito nel *Codice di autoregolamentazione Internet e minori*, «specifiche misure a tutela dei minori nella fascia oraria di programmazione compresa tra le ore 16 e le ore 19» (c.d. "fascia protetta") e a contrassegnare con un segnale di avvertimento i programmi destinati al pubblico adulto. Più precisamente, l'art. 37 del TUSMA vieta le trasmissioni che, anche in relazione all'orario di messa in onda, possano nuocere allo sviluppo fisico o psichico dei minori. Sono altresì vietate scene di violenza gratuita o insistita o efferata, ovvero pornografiche; inoltre, le trasmissioni non debbono contenere programmi vietati ai minori di anni quattordici a meno che la scelta dell'orario di trasmissione, fra le ore 23 e le ore 7, o qualsiasi altro accorgimento tecnico, escludano che i minori vedano o ascoltino normalmente tali programmi; qualora tali programmi siano trasmessi, nel caso di trasmissioni radiofoniche devono essere preceduti da un'avvertenza acustica e, in caso di trasmissioni televisive, devono essere identificati, per l'intera durata della trasmissione, da un simbolo visivo chiaramente percepibile e riconoscibile dall'utente.

coinvolgimento esprime ancora una volta la strategia europea che mira alla valorizzazione del metodo di co-regolazione al quale si è fatto riferimento nelle pagine precedenti.

Ai sensi dell'art. 42, comma 3 del TUSMA, l'AGCOM promuove forme di co-regolamentazione e di autoregolamentazione anche attraverso altri codici di condotta, nel rispetto di quanto previsto dagli articoli 4-bis e 28-ter della direttiva 2010/13/UE, come modificata dalla direttiva 2018/1808/UE. Secondo il disposto del richiamato articolo del TUSMA, i codici di condotta, una volta approvati, devono essere comunicati senza indugio all'Autorità, che è tenuta a verificarne la conformità alla legge e ai propri atti regolatori e ad approvarli, dopodiché è chiamata al controllo sulla loro attuazione (v. anche art. 42, commi 4 e 5, TUSMA)⁹. Pertanto, oltre che svolgere attività preparatorie e istruttorie, all'Autorità per le Garanzie nelle Comunicazioni spetta anche la vigilanza sull'osservanza delle norme del TUSMA e la funzione sanzionatoria, in collaborazione con il Comitato di applicazione del *Codice di autoregolamentazione media e minori*.

6 TRE VIE DA PERCORRERE PER L'INCREMENTO DELLA PROTEZIONE *ONLINE*: MECCANISMI DI *PARENTAL CONTROL*, EDUCAZIONE DIGITALE E COLLABORAZIONE TRA LE *AUTHORITIES*

Come già accennato, l'art. 42 del TUSMA impone ai fornitori di servizi media l'obbligo di dotarsi di sistemi di controllo parentale, ossia di *software* che permettono ai genitori di controllare e bloccare o limitare l'accesso a contenuti inadatti o a determinate attività da parte del minore e di impostare il tempo di utilizzo del dispositivo elettronico da parte dello stesso. Questi filtri si installano mediante la creazione di un profilo utente del minore, dal quale lo stesso potrà connettersi alla rete.

A tale riguardo, nel 2020, il Governo italiano ha introdotto nella formulazione dell'art. 7 bis del decreto-legge n. 28 del 30 aprile 2020 (convertito in l. 25 giugno 2020 n. 70, in materia di "Sistemi di protezione dei minori dai rischi del cyberspazio") l'obbligo per diversi soggetti - tra cui gli operatori di telefonia e i fornitori di altre comunicazioni elettroniche - di attivare "sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto". Allo scopo

⁹ In caso di violazione di quanto disposto dall'art. 42 del TUSMA, si applicano le sanzioni amministrative di cui all'articolo 67, comma 9, salvo quanto previsto dall'art. 74 del Regolamento (UE) 2022/2065 per le violazioni delle disposizioni recate dal medesimo regolamento europeo (art. 42, comma 10, TUSMA). Ferma restando la possibilità di ricorrere all'Autorità giudiziaria, per la risoluzione delle controversie derivanti dall'applicazione dell'art. 42 del TUSMA, è ammesso il ricorso alle procedure alternative e stragiudiziali di risoluzione delle controversie fra utenti e fornitori, nel rispetto del decreto legislativo 4 marzo 2010, n. 28, da un apposito regolamento adottato dall'AGCOM (art. 42, comma 9, TUSMA).

di dare attuazione a questa disposizione, l’Autorità per le Garanzie nelle Comunicazioni, con delibera n. 9 del 25 gennaio 2023 ha adottato Linee guida per i contratti con i consumatori, che impongono ai fornitori di servizi di accesso a Internet, a prescindere dal tipo di tecnologia utilizzata, l’obbligo di attivare strumenti idonei a filtrare automaticamente i contenuti inappropriati.

La delibera AGCOM n. 9/2023, inoltre, fornisce un elenco dei principali siti nocivi per i minori, tra cui quelli aventi contenuti pornografici o quelli che promuovono il gioco d’azzardo o la vendita di armi o quelli che inducono alla violenza, all’odio, alla discriminazione, a pratiche pregiudizievoli per la salute o i siti che suggeriscono modalità per rendere non rintracciabile un’attività *online*.

Molte compagnie telefoniche già predispongono nelle Sim degli *smartphone* sistemi di *parental control* a pagamento, ma la delibera AGCOM n. 9/2023 ne prevede la gratuità: tali sistemi debbono essere inclusi nei contratti tra operatori di telefonia e consumatori senza alcun costo, mentre, nel caso di contratti intestati ai minorenni, debbono risultare già pre-attivati all’interno del dispositivo; sì che solo i maggiorenni o gli esercenti la responsabilità genitoriale possono eseguirne la disattivazione.

L’impianto normativo appena delineato è stato confermato di recente dal Governo italiano con il decreto-legge del 15 settembre 2023 n. 123 (c.d. decreto Caivano), convertito con legge 13 novembre 2023, n. 159, recante «Misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale»¹⁰.

Il complesso di misure prefigurato dalla delibera AGCOM n. 9/2023 e dalla legge di conversione del d.l. 2023 n. 123 è apprezzabile per aver disposto interventi urgenti nel contrasto ai contenuti illegali e per aver indicato le vie da percorrere per il raggiungimento della sicurezza dei minori in ambito digitale.

In primo luogo, atteso che il meccanismo di *parental control* incluso nei contratti con i fornitori entra in funzione solo se attivato dai genitori, emerge il ruolo fondamentale dell’educazione e della formazione degli esercenti la responsabilità genitoriale per un’effettiva tutela dei minori *online*.

¹⁰ L’art. 13 del d.l. 2023 n. 123, al comma 5, fa salva per le offerte di servizi dedicate ai minori la normativa già vigente (posta dal citato art. 7 bis d.l. n. 28 del 30 aprile 2020), la quale prevede l’obbligo del fornitore di pre-attivazione gratuita di un sistema di *parental control*. Lo stesso art. 13 prevede, al comma 1, che i fornitori dei servizi di comunicazione elettronica assicurino gratuitamente (come accessorio al servizio principale) la disponibilità di applicazioni per il controllo parentale nell’ambito dei contratti di fornitura dei servizi elettronici. Si dispone che, entro un anno dall’entrata in vigore del decreto (quindi, entro il 16 settembre 2024), i produttori debbano assicurare, al momento dell’immissione sul mercato dei dispositivi, che i sistemi operativi ivi installati consentano l’utilizzo di applicazioni per il controllo parentale.

Sotto questo profilo, il legislatore italiano impone ai produttori dei dispositivi di comunicazione elettronica di informare dell'importanza di installare applicazioni di controllo parentale, tramite l'inserimento, nelle confezioni di vendita, di uno specifico foglio illustrativo (v. art. 13, comma 3, d.l. 2023, n. 123). In particolare, l'art. 14 del d.l. 2023, n. 123 (*Alfabetizzazione digitale e mediatica a tutela dei minori e campagne informative*) dispone che la Presidenza del Consiglio dei ministri - *Dipartimento per le politiche della famiglia* - elabori Linee guida rivolte ai fruitori di dispositivi di comunicazione elettronica e di applicazioni di controllo parentale, con particolare attenzione agli educatori, alle famiglie e ai minori stessi. I Centri per la famiglia di cui all'art. 1, comma 1250, lett. e), della legge 27 dicembre 2006, n. 296, devono offrire consulenza e servizi in merito alla alfabetizzazione mediatica e digitale dei minori, con specifica attenzione alla loro esposizione a contenuti pornografici e violenti. A tal fine, il *Ministro per la famiglia, la natalità e le pari opportunità* è chiamato ad individuare, di intesa con il Ministero *made in Italy*, i criteri e le modalità di attuazione di «campagne di informazione sull'uso consapevole della rete e sui rischi connessi, in particolar modo sui mezzi di prevenzione dall'accesso a contenuti potenzialmente nocivi per lo sviluppo armonioso dei minori»¹¹.

Quanto alle limitazioni all'accesso a Internet, il d.l. 2023 n. 123 prevede che i gestori dei siti web che diffondono in Italia immagini e video a carattere pornografico sono tenuti a verificare la maggiore età degli utenti (art. 13 *bis*, d.l. 2023 n. 123). La limitazione all'accesso dei minori ai contenuti inadeguati risulta, tuttavia, vincolata dalla rete telefonica e, perciò, potrebbe essere facilmente elusa attraverso il collegamento del dispositivo elettronico ad una rete Wi-Fi (si pensi, ad esempio, all'utilizzo di servizi, come VPN, che permettono di bypassare il blocco dei siti potenzialmente dannosi).

In definitiva, allo stato attuale, anche i sistemi di *age verification* implementati dalle piattaforme si sono dimostrati fallaci. Un supporto per risalire all'età di chi accede alla rete può rinvenirsi nei sistemi di identificazione biometrica, che, se impiegati nel rispetto della normativa sulla *privacy*, permettono di individuare l'utente sulla base di una o più caratteristiche biologiche (riconoscimento facciale, impronta digitale, voce, ecc.) decifrate mediante algoritmi. Un altro metodo, attualmente in fase di sperimentazione, è quello che

¹¹ Per espressa previsione, L'AGCOM, entro il 31 gennaio di ciascun anno, deve predisporre una relazione sullo stato di attuazione della norma relativa all'utilizzo dei *parental control* e alla verifica della maggiore età per l'accesso a siti pornografici, da inviare all'*Autorità politica con delega alle politiche per la famiglia*; tale Autorità politica, entro il 31 maggio di ciascun anno, è tenuta a presentare una relazione al Parlamento, basata anche su ulteriori elementi acquisiti nell'ambito dell'Osservatorio per il contrasto della pedofilia e della pornografia minorile, dell'Osservatorio nazionale per l'infanzia e l'adolescenza, operanti presso il Dipartimento per le politiche della famiglia della Presidenza del Consiglio dei ministri, e dell'Osservatorio sul fenomeno della violenza domestica.

pone, quale condizione di accesso ai servizi elettronici, l'identificazione del minore tramite SPID, il cui rilascio può essere richiesto dai genitori che risultano già muniti dei propri fascicoli sanitari elettronici¹². Per questa via, le potenzialità dell'Intelligenza Artificiale verrebbero sfruttate per garantire la conformità ai principi e il rispetto delle regole. Andrebbe, pertanto, valorizzata la loro capacità di identificare in anticipo meccanismi in grado di intercettare le attività illecite e fraudolente. In questa direzione dovrebbe muoversi l'AGCOM, alla quale è stato attribuito il potere di stabilire con proprio provvedimento, previo parere del Garante per la *privacy*, le modalità tecniche che le piattaforme sono tenute ad adottare per accertare la maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e rispettando la minimizzazione dei dati personali raccolti in ragione dello scopo (v. art. 13 *bis* del d.l. 2023 n. 123)¹³. Sempre con proprio provvedimento, l'AGCOM è chiamata a definire le procedure e le modalità operative per l'esercizio dei suoi poteri e a gestire in modo autonomo le risorse finanziarie necessarie per svolgere i propri compiti (v. comma 3 dell'art. 15 del d.l. 2023 n. 123).

Dopo circa venti anni dall'adozione del *Codice di autoregolamentazione Internet e minori*, il *Comitato media e minori* non è più l'unica autorità governativa in materia, data la configurazione di un rinnovato meccanismo di vigilanza pubblica, imposto a livello sia nazionale che sovranazionale. Questo rappresenta una via maestra, di fronte a eventuali carenze di famiglia, scuola e società in genere, per garantire una tutela effettiva ai minori. Le pubbliche Autorità c.d. indipendenti, garanti dei diversi settori (Autorità Garante per le Comunicazioni Autorità Garante per la protezione dei dati personali, Autorità Garante per la concorrenza ed il mercato, ecc.), possono attivare diverse misure cautelari per far cessare in via immediata le condotte illecite sul web o, meglio, per prevenirle ancor prima che vengano commesse. Le attribuzioni delle Autorità indipendenti sono in aumento, come risulta dai recenti Regolamenti europei sui servizi digitali: nuovi soggetti pubblici vengono istituiti,

¹² In base a tale sistema, l'*Internet service provider* – es. Poste Italiane – fornisce ai genitori lo SPID per il figlio; così accerta l'età del figlio per poi inviare al *social network* una stringa di testo che indica se lo stesso può accedere alla piattaforma in base all'età. Si veda, al riguardo, Agenzia per l'Italia digitale (Agid), *Linee guida operative per la fruizione dei servizi SPID da parte dei minori*, marzo 2022 (reperibile nel sito: <https://trasparenza.agid.gov.it/>).

¹³ Il d.l. 2023 n. 123 dispone che, entro sei mesi dalla data di pubblicazione del provvedimento dell'AGCOM, le piattaforme debbano dotarsi di efficaci sistemi di verifica della maggiore età conformi alle prescrizioni impartite nel provvedimento stesso. Spetterà poi sempre all'AGCOM vigilare sulla corretta applicazione di detta disposizione e, in caso di inadempimento, contestare la violazione alle piattaforme, anche d'ufficio, diffidandole ad adeguarsi entro venti giorni. In caso di inottemperanza alla diffida, l'AGCOM dovrà adottare ogni provvedimento utile per il blocco del sito o della piattaforma fino al ripristino di condizioni di fornitura conformi ai contenuti della diffida.

mentre le Autorità già esistenti vedono dilatare le loro funzioni, che sono di regolazione, oltre che di controllo e giudicanti, interdittive, conformative e sanzionatorie¹⁴.

Il protagonismo in Italia e in Europa di dette Autorità evidenzia le strette interrelazioni, nelle e-agorà, tra tutela dei consumatori, tutela della concorrenza e protezione della riservatezza, settori chiave, che normalmente vengono tenuti distinti e che, invece, nel mercato digitale si intrecciano necessariamente, per realizzare la piena tutela dei bisogni di ogni contraente debole e, in particolare, del contraente minore d'età. Le *Authorities* perseguono obiettivi diversi, ma sono chiamate ad operare insieme, soprattutto per operare un bilanciamento tra il diritto alla protezione dei minori e l'esigenza di disporre di un'ingente mole di dati per lo sviluppo del mercato e delle nuove tecnologie.

In considerazione delle funzioni già da essa svolte nel campo delle comunicazioni elettroniche, dei media e dei servizi digitali, l'AGCOM è stata individuata dall'art. 15 del d.l. 2023 n. 123 come *Coordinatore dei servizi digitali* in attuazione dell'art. 49, comma 2, del *Digital Services Act*. Secondo tale disposizione, in ciascuno Stato membro, i Coordinatori dei Servizi Digitali devono cooperare tra loro e con le altre autorità nazionali competenti, con il Comitato europeo dei coordinatori nazionali e con la Commissione europea. L'AGCOM è, dunque, chiamata a collaborare con ogni altra Autorità competente, svolgendo i propri compiti in modo imparziale, trasparente e tempestivo. Sia a livello europeo che a livello nazionale, la cooperazione tra le autorità competenti nei vari settori può esplicarsi in vari modi, anche sottoscrivendo protocolli di intesa per disciplinare gli aspetti applicativi e procedurali di ciascuna attività, ovvero attraverso periodici scambi di opinioni e mediante comunicazione reciproca in merito alle indagini in corso.

Si auspica che in futuro il complesso di misure introdotte a livello italo-europeo sia in grado di raggiungere l'obiettivo di assicurare un *enforcement* effettivo dei diritti digitali a tutte le persone, inclusi i minori.

REFERÊNCIAS

BELLELLI, A. 2014. Il problema della giuridicità delle regole deontologiche delle professioni. In: M. NUZZO (a cura di). *Il principio di sussidiarietà nel diritto privato*. Torino: Giappichelli.

¹⁴ In base al Considerando 112 del *Digital Service Act*, l'AGCOM deve agire in piena indipendenza da enti privati e pubblici. L'indipendenza delle *Authorities* non significa che i loro provvedimenti non siano soggetti al controllo di costituzionalità e non vuol dire che sia impedito il controllo giurisdizionale o la possibilità di consultare altre autorità nazionali, incluse le autorità giudiziarie; implica soltanto che esse non sono obbligate a ricevere istruzioni da terzi e neppure dai governi nazionali.

- BELLELLI, A. 2023. Soft-law e co-regolazione. *In: R. BOCCHINI (a cura di). Manuale di diritto privato dell'informatica*. Napoli: Edizioni Scientifiche Italiane.
- BERTI DE MARINIS, G. 2016. Autodeterminazione e capacità di discernimento del minore: profili di diritto civile. *Actualidad Jurídica Iberoamericana*, **50**.
- BIANCA, C.M. 2002. *La norma giuridica, I soggetti. Diritto civile*, 1; Milano: Giuffrè.
- BOCCHINI, F. 2000. L'interesse del minore nei rapporti patrimoniali. *Rivista diritto civile*. (1):277.
- BOCCHINI, R. 2019. Responsabilità civile dell'hosting provider – la responsabilità civile, plurisoggettiva, successiva ed eventuale dell'ISP. *Giurisprudenza italiana*.
- CINQUE, M. 2007. Il minore e la contrattazione telematica tra esigenze del mercato e necessità di apposite tutele. *Nuova giurisprudenza civile commentata*. (1):2019.
- CITARELLA, V. 2023. La tutela dei minori per la prevenzione ed il contrasto del fenomeno del Cyberbullismo. *In: R. BOCCHINI (a cura di). Manuale di diritto privato dell'informatica*. Napoli, Edizioni Scientifiche Italiane.
- COLOMBO, C. e BRESSLER, C. 2022. *In: AC.B. TEIXEIRA; J.L.M. FALEIROS; R. DENSA (Org.). Infância, Adolescência e Tecnologia: O Estatuto da Criança e do Adolescente na Sociedade da Informação*. Indaiatuba, Foco. 243-266.
- DI SABATO, D. 2020. Il ruolo delle piattaforme digitali nello svolgimento delle attività economiche in rete. *Annali della Facoltà Giuridica dell'Università di Camerino – Studi*.
- DOSI G. 1995. Dall'interesse ai diritti del minore: alcune riflessioni. *Diritto di famiglia e delle persone*, 1604.
- GAMBINO, A.M. 2015. I contratti di accesso. *In C. Perlingieri e L. Ruggeri (a cura di). Internet e diritto civile*. Napoli: Edizioni Scientifiche Italiane.
- GIARDINA, F. 1984. *La condizione giuridica del minore*. Napoli: Jovene.
- GIOVA, S. 2014. La tutela del consumatore telematico nel d.lgs. n. 21 del 2014. *Rivista giuridica Molise Sannio* (3):109.
- GIOVA, S. 2023. La persona nel contesto digitale: considerazioni conclusive. *Tecnologie e diritto* (2):323.
- LIPARI, N. 1987. La formazione negoziale del diritto. *Rivista diritto civile*. (1):307.
- MEZZASOMA, L., RIZZO, V., RICCIUTO, V. e LLAMAS POMBO, E. (a cura di). 2016. *Il consumatore di servizi tra Italia, Spagna e Latino America*. Napoli: Edizioni Scientifiche Italiane.
- PERLINGIERI, C. 2014. *Profili civilistici dei social networks*. Napoli: Edizioni Scientifiche Italiane.

PERLINGIERI, C. 2016. La tutela dei minori di età nei “social networks”. *Rassegna diritto civile*.

PERLINGIERI, G., MEZZASOMA L., ANGELONE M. (a cura di). 2024. *Manuale di diritto dei consumi*. Napoli: Edizioni Scientifiche Italiane.

PERLINGIERI, P. 2018. Privacy digitale e protezione dei dati personali tra persona e mercato. *Foro napoletano*, **3**.

PIEPOLI, G. 1997. Autodisciplina professionale e codici deontologici, una prospettiva europea. *Quaderni diritto privato europeo*. (1):85.

RESCIGNO, P. 1988. Capacità di agire. *Digesto Encyclopedia. Discipline privatistiche, Sezione civilistica*.

SENIGAGLIA, R. 2022. *I principi e le categorie del diritto civile minorile*. In A. Cordiano e R. Senigaglia (a cura di). *Diritto civile minorile*. Napoli: Edizioni Scientifiche Italiane.

STANZIONE, P. 1980. Potestà dei genitori e diritti fondamentali del minore. *Rassegna diritto civile*. (1):460.

VACCÀ, C. (a cura di). 1999. *Il commercio elettronico: il documento digitale, internet, la pubblicità online*. Milano: EGEA.

VALONGO, A. 2014. *Deontologia medica e regole di responsabilità alla luce del principio di sussidiarietà*. In M. Nuzzo (a cura di). *Il principio di sussidiarietà nel diritto privato*. Torino: Giappichelli. (1): 157.

ZAGREBELSKY, G. 1992. *Diritto mite*. Torino: Einaudi.