

DENISE
AMRAM

NON HO L'ETÀ, MA...

COSTRUIRE COMPETENZE ABILITANTI
PER UNA SOCIETÀ DELL'INFORMAZIONE
A PROVA DI (IN)CAPACITÀ DEL MINORE DI ETÀ



Lefebvre Giuffrè

DENISE
AMRAM

NON HO L'ETÀ, MA...

**COSTRUIRE COMPETENZE ABILITANTI
PER UNA SOCIETÀ DELL'INFORMAZIONE
A PROVA DI (IN)CAPACITÀ DEL MINORE DI ETÀ**



Lefebvre Giuffrè

ISBN 9788828877769

Il presente volume è stato sottoposto a referaggio

Il volume è stato realizzato con il cofinanziamento dell'Unione europea - Next Generation EU; CUP: J53D23005540006, nell'ambito del progetto PRIN 2022 "*Children as Vulnerable users of IoT and AI-based technologies: a multi-level and interdisciplinary approach*" (CURA) - CAKAEWYF".

FSC

© Copyright Giuffrè Francis Lefebvre S.p.A. Milano - 2025
Via Monte Rosa, 91 - 20149 MILANO - www.lefebvregiuffre.it

La traduzione, l'adattamento totale o parziale, la riproduzione con qualsiasi mezzo (compresi i microfilm, i film, le fotocopie), nonché la memorizzazione elettronica, sono riservati per tutti i Paesi.

Stampato da LegoDigit s.r.l. - Lavis (TN)

A Mélanie, Paride e Fabio

UNA PREMESSA

Nel 2019 durante un pranzo con amici e conoscenti mi colpì una conversazione con una bambina di dieci anni circa che giocava con il cellulare della madre: stava caricando nel completo silenzio-assenso dei genitori video di balletti con altri commensali suoi coetanei su una nota piattaforma *social*. Mi chiese il permesso di postarne uno assieme a mia figlia di cinque anni. Le chiesi come funzionasse la piattaforma e mi rispose che, sebbene il profilo fosse suo, l'*account* era stato registrato a nome della mamma, che aveva dovuto acconsentire all'iscrizione. Negai il permesso a condividere un video che ritraeva anche mia figlia, le spiegai che non ritenevo necessario rendere pubblico il ricordo della giornata trascorsa assieme, non potendo prevedere cosa ne sarebbe stato di quel video il giorno dopo e quello successivo ancora. La bambina obbedì senza comprendere troppo il motivo del mio rifiuto. La mamma la liquidò dicendo che, essendo “avvocato”, ero rigida sulle questioni di *privacy*.

Percepì una distanza culturale ed educativa, non tanto dalla bambina, come era ovvio, ma dalla mamma. Capii che c'era un disallineamento di visioni e di percezione dei rischi rispetto alla dimensione digitale. Compresi che la causa fosse da attribuire in primo luogo al vuoto legislativo: nessuna norma della società dell'informazione e nessun dibattito sull'affidabilità delle nuove tecnologie si occupavano invero della particolare posizione del bambino-utente dei servizi e dei prodotti digitali.

Da allora, ho avuto modo di confrontarmi con altri studiosi, di diverse discipline, che avevano provato lo stesso disagio ad osservare l'evidente discrepanza fra le grandi opportunità lanciate dalla trasformazione digitale, da un lato, e l'inerzia delle iniziative di politica del diritto, ancor prima che legislative, rispetto alla protezione e promozione dei diritti dei fanciulli nella nuova dimensione, dall'altro.

Eppure le nuove generazioni sono quelle native digitali e sono il nostro futuro.

Eppure il progresso scientifico-tecnologico porta quotidianamente

a dover affrontare nuove sfide, impattando in misura sempre diversa sulla realizzazione della persona.

Oggi l'attenzione è cresciuta, seppur in ritardo e con interventi non sempre organici ed efficaci, ma si percepiscono bisogni di tutela e di valorizzazione comuni, pressoché universali, tra gli utenti minori di età, cui corrispondono meccanismi di responsabilizzazione degli adulti, degli operatori economici e delle istituzioni spesso carenti e lacunosi.

Un ulteriore profilo mi ha incuriosito negli anni vedendo mia figlia crescere e sviluppare abilità e competenze tecnologiche che io stessa ho appreso solo da adulta, peraltro non senza riluttanza e fatica: quello della valorizzazione delle opportunità offerte dall'innovazione ai giovani utenti. Mi son allora tornate alla mente le parole del professor Francesco Donato Busnelli, che ci ha sempre sollecitato a leggere le categorie giuridiche attraverso la lente della promozione della dignità della persona: "*Minore?! È un termine che non mi piace: minore rispetto a chi? A cosa?*".

È per tali ragioni che con questo modesto contributo abbiamo provato a fare ordine fra le fonti normative e a proporre un modello che promuova la crescita personale e culturale, prima ancora che l'adozione di specifiche misure tecnico-organizzative, e che possa sia nelle piccole comunità, sia nelle grandi realtà, costruire spazi digitali e tecnologie a misura di bambini e adolescenti.

Un sincero ringraziamento va alla Scuola Superiore Sant'Anna e a tutte le sue componenti per il quotidiano supporto scientifico-culturale e tecnico-amministrativo alle mie iniziative di ricerca, didattiche e di terza missione, con l'augurio di continuare assieme a immaginare opportunità e soluzioni per una società più inclusiva e solidale.

Pontedera - Pisa, 2 agosto 2024 - 11 aprile 2025

INDICE SOMMARIO

Una premessa	VII
------------------------	-----

INTRODUZIONE

LA DATIFICAZIONE DELLA SOCIETÀ E I BAMBINI	1
--	---

CAPITOLO I

DATIFICAZIONE DELLA SOCIETÀ E NUOVE TECNOLOGIE: LEGGERE IL QUADRO REGOLATORIO ATTRAVERSO LE LENTI DEI MINORI DI ETÀ

1. Il quadro regolatorio: governare la dimensione digitale e le nuove tecnologie tra rischi e opportunità	19
2. Il Regolamento europeo sulla protezione dei dati personali e la questione relativa all'età per esprimere un valido consenso	22
2.1. I minori di età, la protezione dei dati e il caso Open AI	28
3. Gratuità e affidabilità: quali strumenti di tutela per gli utenti inconsapevoli?	30
4. Il Regolamento europeo sui servizi digitali: gli obblighi di trasparenza . .	36
4.1. (<i>Segue</i>). Gli obblighi di protezione per i minori di età	38
5. Le ricadute su specifiche normative di settore: il Regolamento sui mercati digitali	43
5.1. (<i>Segue</i>). La regolamentazione dei contenuti audiovisivi	45
6. (<i>Segue</i>). Il dibattito sulla regolamentazione dei neurodiritti	48
7. La regolamentazione UE per lo sviluppo di sistemi IA affidabili.	52
7.1. (<i>Segue</i>). L'intelligenza artificiale a portata dei minori di età: i lavori dell'UE e del Consiglio d'Europa a partire dalle raccomandazioni elaborate dall'UNICEF	63
8. La regolamentazione della società dei dati nei sistemi extra-UE	72
8.1. I sistemi di <i>Common Law</i>	74
8.2. Il <i>Digital Charter Implementation Act canadese</i> e il Codice civile del Québec.	76
8.3. L'approccio negli USA e le iniziative statali: cenni.	79
9. I sistemi tecnologicamente avanzati in Asia e Oceano Pacifico	81

9.1.	La tutela dei dati personali “adeguata” in Corea del Sud e Giappone e i relativi approcci verso i minori di età	83
9.2.	Il sistema cinese: cenni e rinvio.	86
9.3.	Il <i>Digital Personal Data Protection Act</i> indiano	87
10.	Le strategie a portata di bambini e adolescenti nei sistemi sudamericani .	90
10.1.	(Segue). Perù	91
10.2.	(Segue). Argentina	93
10.3.	(Segue). Il sistema di tutele in Brasile e la risoluzione “settoriale” (cenni e rinvio)	95
11.	I sistemi africani: cenni alle misure introdotte in Swaziland, Uganda e Ruanda	101
12.	Regolamentare la società dell’informazione e le nuove tecnologie per i minori di età: osservazioni di sintesi	104

CAPITOLO II

PROTEGGERE I DIRITTI FONDAMENTALI DEI BAMBINI NELLA DIMENSIONE DIGITALE: LE MISURE TECNICO-ORGANIZZATIVE PER LA MITIGAZIONE DEI RISCHI

1.	I diritti fondamentali del fanciullo: la dimensione digitale della CRC . . .	111
1.1.	(Segue). I rischi nella dimensione digitale e le responsabilità multilivello.	114
2.	Il sistema di tutele sui prodotti: il precedente delle direttive CE sulla sicurezza dei giocattoli e la nuova direttiva UE sui prodotti difettosi . . .	118
3.	Gli approcci nazionali e le implicazioni di sistema.	122
3.1.	Le misure volte a proibire l’accesso ai minori a determinati servizi: il dibattito negli USA e in Australia	123
3.2.	Le misure a portata dei bambini dell’ <i>Online Safety Act</i> : il pragmatismo britannico.	129
3.3.	La riforma cinese e l’autonomia c.d. limitata	133
4.	La protezione dei fanciulli <i>by design</i> e il ruolo degli <i>standard</i> tecnici . . .	137
5.	La valutazione di impatto con le lenti dei diritti dell’infanzia e il problema tecnico della verifica dell’età	142
6.	Sviluppare un sistema di tutele nell’ordinamento italiano a partire dalle esperienze straniere.	149
6.1.	(Segue). Le responsabilità genitoriali nella dimensione digitale . . .	151
6.2.	(Segue). Verso un patentino per l’utente minorenne?	155
7.	Dalla protezione alla promozione dei diritti fondamentali nella dimensione digitale (cenni e rinvio).	156

CAPITOLO III

**DIRITTI UNIVERSALI E VULNERABILITÀ MULTIPLE:
PROMUOVERE IL BENESSERE DI TUTTI I MINORI
DI ETÀ NELLA DIMENSIONE DIGITALE**

1.	Diversità, inclusione e il diritto all'accesso alle risorse	160
1.1.	(Segue). Le vulnerabilità multiple...	163
1.1.1.	(Segue). ...e il settore educativo.	165
1.1.2.	(Segue). ...e il settore sanitario	170
2.	Muoversi attorno al piano dell'autonomia e della consapevolezza del singolo: il ruolo della trasparenza.	174
3.	L'educazione digitale: rafforzare conoscenze e competenze tecnologiche .	178
4.	Nuove tecnologie, gioco e creatività	181
5.	Promuovere la sfera relazionale e quella emotiva.	184
6.	L'identità digitale e il problema della costruzione della reputazione. . . .	187
7.	La prospettiva partecipativa nella dimensione digitale.	190
8.	La responsabilizzazione delle istituzioni e degli operatori economici . . .	193
8.1.	(Segue). La responsabilizzazione degli adulti e delle comunità di riferimento per il minore	194
9.	Costruire una dimensione digitale assieme a (e alla portata di) bambini e adolescenti.. . . .	196
9.1.	(Segue). ...e le considerazioni di sistema	200
9.2.	La declinazione dei cc.dd. <i>best interests of the child</i> e gli spazi di "adattamento".	205
9.2.1.	L'approccio anagrafico e orientato alla trasparenza	208
9.2.2.	L'approccio a partecipazione consapevole e personalizzata .	214
9.2.3.	La combinazione dei due approcci	217

NOTE CONCLUSIVE

**LA MITIGAZIONE DELLE VULNERABILITÀ NELLA SOCIETÀ
DELL'INFORMAZIONE: COSTRUIRE COMPETENZE
E PROMUOVERE TUTELE A GEOMETRIA VARIABILE**

1.	L'approccio basato sulla valutazione del rischio e il sistema di tutele a geo- metria variabile volto alla costruzione di competenze	219
2.	Decostruire l'incapacità: mitigare le vulnerabilità del minore, costruendo competenze e abilità	225
3.	Non ho l'età, ma... ho il patentino: circolazione del modello e implicazioni sui paradigmi di responsabilità.. . . .	232
4.	(Segue). ... interessi superiori, (in)capacità e dignità del minore di età. . .	235

<i>Bibliografia.</i>	239
--------------------------------	-----

INTRODUZIONE

LA DATIFICAZIONE DELLA SOCIETÀ E I BAMBINI

1. La datificazione della società ⁽¹⁾ ha costruito nuove lenti attraverso cui interpretare la realtà: l'analisi dei dati, o meglio, delle grandi moli di dati, consente oggi di comprendere la società da una prospettiva più oggettiva, basata sulle aggregazioni statistiche, che permettono di identificare correlazioni tra diversi fenomeni e risolvere i problemi, avendo una visione più ampia dell'insieme delle problematiche e delle variabili che possono impattare su un certo profilo investigato.

Il ciclo di vita dell'informazione è oggi parte integrante, se non dominante, nello sviluppo di nuova conoscenza: raccolta ed elaborazione di basi di dati costituiscono meccanismi essenziali per descrivere, valutare e monitorare un fenomeno naturale o artificiale. Nessun settore è escluso: dall'agricoltura, all'industria, ai servizi erogati sia dalle pubbliche amministrazioni, sia dalle aziende private, o da professionisti, sia per finalità di lucro o per spirito di liberalità.

Si parla di società dell'informazione ⁽²⁾ proprio per definire questo particolare momento storico ove ogni processo decisionale — automatizzato o meno — trova evidenza nel dato elaborato. A sua volta, però, ogni attività di trattamento finalizzata ad un processo decisionale deve poter essere giustificata alla luce dei valori condivisi attualmente dalla e nella società civile. Di conseguenza, la riflessione sull'attualità delle interpretazioni di fatti o condotte rispetto ai principi informatori della materia e alle categorie del diritto esistenti richiede un confronto

⁽¹⁾ Tra i primi a descrivere le implicazioni sociali della società dell'informazione: M. CASTELLS, *The Rise of the Network Society*, The Information Age: Economy, Society and Culture Vol. I, 1996, Cambridge, MA; Oxford, UK: Blackwell, Id., *The Power of Identity*, The Information Age: Economy, Society and Culture Vol. II, 1997, Cambridge, MA; Id., *End of Millennium*, The Information Age: Economy, Society and Culture, Vol. III, 1998.

⁽²⁾ V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2003, p. 89 ss.

costante con il sostrato sociale, ciò al fine di costruire un robusto apparato di tutele attraverso misure di salvaguardia che effettivamente mettano al centro la dignità delle persone e i relativi bisogni.

La rapidità con cui la scienza dei dati pone nuovi dilemmi e nuovi quesiti giuridici, invero, provoca il proliferarsi di posizioni estemporanee volte, da un lato, a dare soluzioni adattabili ad un caso concreto e difficilmente replicabili in contesti diversificati; dall'altro lato, a discutere in maniera del tutto astratta rispetto alle effettive (vecchie e nuove) vulnerabilità e al relativo declinarsi in una dimensione diversa, quale quella promossa dall'elaborazione dei dati ⁽³⁾.

Di fronte a questo scenario, gli addetti ai lavori (*i.e.* i prestatori di servizi digitali, gli sviluppatori o fornitori di nuove tecnologie, più in generale gli operatori economici) chiedono strumenti interpretativi, regole di diligenza e *standard* tecnici da applicare alla moltitudine di scenari che anche una singola organizzazione può sviluppare, mentre le strategie regolatorie dell'Unione Europea adottano la logica della rendicontazione, sulla base del principio di *accountability*, individuando — generalmente — una matrice di ruoli e responsabilità, cui allocare l'obbligo di percepire eventuali rischi e implementare misure di contenimento per proteggere caso per caso non solo ogni singolo utente, ma — più in generale — la persona umana e i relativi diritti fondamentali ⁽⁴⁾.

Tale approccio del legislatore europeo deriva dalla strategia politico-economica ispirata al principio di precauzione ⁽⁵⁾, volta a fornire

⁽³⁾ “Cambia l'epistemologia del giurista, overosia il modo in cui egli organizza le regole, (...) Il cambio di passo mentale consiste nel passaggio da una logica essenzialmente causale, in cui l'argomentazione — e dunque la concatenazione delle regole — segue un ragionamento consequenziale, ad una logica di tipo inferenziale”, così V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2018, p. 37.

⁽⁴⁾ J. SHAHIN - M. FINGER, *The History of a European Information Society: Shifts from governments to governance*, in J. TUBTIMHIN - R. PIPE (a cura di), *Global e-Governance: Advancing governance through innovation and leadership*, Amsterdam, IOS Press, 2009, Global E-Governance Series, Vol. 2, 62-83 che richiamano il precedente R. HAWKINS, *Standards for Communication Technologies: Negotiating Institutional Biases in Network Design*, in R. MANSELL - R. SILVERSTONE (a cura di), *Communication by Design: The Politics of Information and Communication Technologies*, 1996, Oxford: Oxford University Press, p. 157 ss.

⁽⁵⁾ Il principio di precauzione è stato enunciato nell'ambito della Conferenza delle Nazioni Unite su ambiente e sviluppo, Dichiarazione di Rio de Janeiro ed i “rischi ambientali”, 1992 e successivamente interpretato come approccio a “un diritto progno-

strumenti e regole, ovvero “*elementi di fatto, idonei a promuovere norme giuridiche (ideologie, valori) (...) all’opera per la creazione di un diritto muto*” ⁽⁶⁾ al fine di non nuocere il prossimo di fronte a un fenomeno — come quello della datificazione della società — in continua evoluzione, il cui impatto sul singolo e sulla collettività non è sempre spiegabile integralmente.

Assistiamo ad una fase in cui gli attori della società dell’informazione si fanno portatori di “*un programma (indefinito ma tuttavia vincolante)*” ⁽⁷⁾ che trova nell’approccio dal basso, basato sulla valutazione (e relativa mitigazione) del rischio percepito, la cornice entro cui sistematizzare gli istituti giuridici e formulare norme vincolanti che possano soddisfare le esigenze di protezione e promozione dei diritti fondamentali della persona in una pluralità di scenari — noti e non ⁽⁸⁾.

2. Ogni giorno, in questo contesto, il “*dialogo tra diritto e tecnica*” ⁽⁹⁾ si rinnova e si intensifica: la lettura della società e delle relazioni tra consociati attraverso i flussi di dati generati quotidianamente dagli individui ha portato le scienze sociali a servirsi di strumenti tecnologicamente avanzati, anche basati su tecniche di *Machine Learning* per raccogliere e analizzare grandi moli di dati, in tempi sempre più rapidi e con risultati sempre più accurati. Di conseguenza, il metodo di indagine ha subito (e subisce), adattamenti sia in termini di attività organizzative della ricerca al fine di gestire le informazioni, sia in termini di lettura e interpretazione dei risultati delle analisi condotte.

stico, che guarda avanti, fin dove, nel tempo, le previsioni scientifiche permettono di gettare lo sguardo”, così G. ZAGREBELSKY, *Decidere noi della scienza*, in www.repubblica.it, 21 febbraio 2012.

⁽⁶⁾ R. SACCO, *Il diritto muto*, Il Mulino, 2015, p. 77.

⁽⁷⁾ *Ibidem*.

⁽⁸⁾ Si pensi all’impatto delle tecniche di intelligenza artificiale cc.dd. generativa sulla necessità di aggiornare la proposta di regolamento UE in materia: *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD))*(1), riflessioni confluite nel testo infine adottato nel Regolamento UE 13 giugno 2024, n. 1689, che stabilisce regole armonizzate sull’intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull’intelligenza artificiale), G. FINOCCHIARO, *Intelligenza Artificiale. Quali regole?*, Il Mulino, 2024.

⁽⁹⁾ N. IRTI - E. SEVERINO, *Dialogo su diritto e tecnica*, Laterza, 2001.

Da un lato, infatti, la società dell'informazione costituisce un nuovo fenomeno da regolamentare. Dall'altro, gli strumenti offerti dalle legislazioni in materia si prestano a fornire una nuova lente attraverso cui guardare le relazioni fra consociati. Questa correlazione impone, accanto all'introduzione di meccanismi di gestione del ciclo di vita del dato nelle attività di ricerca, un adattamento interdisciplinare alle metodologie di lettura e interpretazione del fenomeno investigato ⁽¹⁰⁾.

Le ricadute sul metodo scientifico sono molteplici, soprattutto in ambito giuridico. In questa prospettiva, ad esempio, istanze di riforma legislativa saranno più efficaci se supportate da analisi statisticamente più rilevanti, purché l'interpretazione dei risultati sia orientata anche a cogliere quelle sfumature la cui portata tenderebbe ad essere ridotta dalla digitalizzazione del processo di analisi ⁽¹¹⁾. In altri termini: se il ruolo dello studioso può considerarsi facilitato dal supporto tecnologico, in ragione della maggiore fruibilità e accesso a risorse e metodi, lo stesso deve tuttavia sviluppare un approccio critico più raffinato per far

⁽¹⁰⁾ In dottrina, si osserva che “*The major difference between land and oil on the one hand and data on the other is that data can be harvested, amassed, and turned into monetary assets without allocating property rights at the outset (...) There is some reason to believe that if every individual held the property rights to her own data, this might create a gridlock, the data harvesters have lobbied hard to obtain legal protection on par with property rights for the aggregate data they have collected effect, because harvesting the data would require prior consent. In practice, this might not be much of a problem given the ease with which consent can be acquired. The European data regulation law, the General Data Protection Regulation (GDPR), is a good example. It requires prior consent from individuals, or an alternative legal basis, for harvesting any personal data (...) This requirement has been translated into an “agree” button for internet users to click whenever they enter a site that uses cookies and similar devices that track their behavior. As it turns out, most internet users do so without hesitation. The consent requirement is a nuisance, but it does not create gridlock. (...) Data harvesters extract the economic value from data not by reselling the aggregate data at a higher price, but by selling the data’s predictive power*” così, K. PISTOR, *Rule by data: the end of markets?*, 2020, *Law and contemporary problems*, Vol. 83:101, p. 108-109, 111.

⁽¹¹⁾ Si pensi alle riflessioni di SANTI ROMANO sull'interpretazione evolutiva, per cui l'interpretazione della norma riflette l'attività cognitiva del singolo: il “*diritto vigente nell'intelletto di chi vuole conoscere tale diritto*” come “*operazione intellettuale che deve potersi compiere nello stesso modo e con gli stessi risultati, anche se con diversa efficacia, sia dal giudice sia da altra autorità sia dai privati, cioè da chiunque può giovare della norma o deve obbedirvi, rispettarla, eseguirla, applicarla, precisarla dottrinalmente*”, in *Frammenti di un dizionario giuridico*, 1947 e alla lettura attuale F. PEDRINI, *Santi Romano e l'interpretazione giuridica. Appunti per una riflessione sul “metodo” nel diritto pubblico*, Jura Gentium, XV (2018), 2, p. 79 ss.

fronte a possibili distorsioni (c.d. *bias*) ⁽¹²⁾ e indirizzarle in ottica costruttiva in termini di politica del diritto senza incorrere nel paradosso di creare regole di fatto inefficaci, in quanto non attuabili o solo formalmente applicabili ⁽¹³⁾.

3. Consapevoli di tali premesse, in questo contributo affrontiamo il tema della protezione e promozione dei diritti dei bambini, quale esempio di utenti vulnerabili della società dell'informazione. L'occasione consente di operare una mappatura delle fonti normative, a partire dalle iniziative dell'Unione Europea, in combinazione con i rischi noti emergenti dalla letteratura e dalle prassi, ed estrarre elementi di politica del diritto capaci di orientare l'interprete rispetto a possibili lacune e paradossi emergenti dal frammentato quadro giuridico di riferimento. La stessa, in ottica necessariamente interdisciplinare, permette altresì di andare a identificare norme operazionali, misure di salvaguardia, sia di tipo tecnico, che organizzativo, in grado di fornire contenuti specifici alle responsabilità distribuite dal legislatore sovranazionale o nazionale ai diversi attori, pubblici o privati.

Con riferimento al sistema italiano, l'analisi intercetta e si collega ad una recente posizione pubblicata dall'Autorità Garante per i Diritti dell'Infanzia e dell'Adolescenza italiana: “*Manifesto dei bambini sui diritti in ambiente digitale*” ⁽¹⁴⁾, che raccoglie dieci principi emersi nell'ambito di uno studio effettuato nelle scuole primarie, previa lettura guidata di un racconto sul tema ⁽¹⁵⁾. In particolare, il Manifesto elabora le percezioni raccolte dai bambini circa il perseguimento del loro benessere nella dimensione digitale, utilizzando un linguaggio semplice, ma facilmente riconducibile a quei diritti che la Convenzione ONU sui diritti dell'Infanzia e dell'Adolescenza (di seguito anche CRC) ⁽¹⁶⁾ riconosce e garantisce e che oggi necessitano di essere

⁽¹²⁾ *Infra* Cap. 1 § 7.

⁽¹³⁾ V. ZENO-ZENCOVICH, *Artificial intelligence, natural stupidity and other legal idiocies*, Editoriale, MediaLaws, 2024.

⁽¹⁴⁾ AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *Manifesto dei bambini sui diritti in ambiente digitale*, 17.3.2023, disponibile a questo indirizzo: <https://www.garanteinfanzia.org/manifesto-dei-bambini-sui-diritti-ambiente-digitale>.

⁽¹⁵⁾ AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *Geronimo Stilton. Alla scoperta del mondo digitale*, realizzato dall'Agia in collaborazione con Piemme - Mondadori Libri, 2022, https://www.garanteinfanzia.org/sites/default/files/2022-05/EducazioneAlDigitale_WEBok.pdf.

⁽¹⁶⁾ Convenzione ONU sui diritti dell'infanzia e dell'adolescenza (Convention on the Rights of the Child, di seguito anche CRC), approvata dall'Assemblea Generale

declinati in sede interpretativa alla luce del progresso scientifico-tecnologico.

In ragione della portata innovativa della dimensione analizzata, una posizione di rilievo è assunta dal diritto all'educazione digitale, declinato come opportunità di far comprendere i rischi dell'uso improprio delle tecnologie, sia ai minori di età, che agli adulti di riferimento, ma non solo. Il Manifesto non manca, infatti, di evidenziare come poter utilizzare applicazioni tecnologiche e accedere ad uno spazio virtuale sicuro costituiscano opportunità irrinunciabili, da garantire a tutti, in maniera inclusiva e senza discriminazioni. Lo stesso richiama — naturalmente — anche la dignità, intesa come espressione del principio personalista, come limite all'autodeterminazione individuale e alla libertà contrattuale non solo dell'interessato, ma in una dimensione relazionale ⁽¹⁷⁾. In questo senso, declinata per assicurare il diritto all'oblio e alla riservatezza rispetto a contenuti condivisi dai minori stessi oggi, laddove per qualsivoglia motivo un domani l'utente decida di dissociarsene o semplicemente non mantenerne memoria. Questo profilo si accompagna alla libertà di esprimere il proprio pensiero, di maturare le proprie convinzioni senza essere discriminato o subire pregiudizi per le proprie affermazioni ⁽¹⁸⁾. Il rispetto delle proprie idee e delle emozioni è orientato affinché non se ne faccia un uso scorretto, che porti a denigrare la persona con fenomeni di violenza, come in caso di cyberbullismo. Infine, il Manifesto si riferisce anche al diritto alla vita privata e familiare, declinato con le lenti dei bambini nel diritto a coltivare “amicizie” e rapporti in “famiglia”, cui si collegano il diritto al gioco in un ambiente sicuro e privo di manipolazioni, da un lato, e quello alla disconnessione, dall'altro, per consentire di sviluppare e

delle Nazioni Unite il 20 novembre 1989 e ratificata dall'Italia il 27 maggio 1991 con la Legge n. 176.

⁽¹⁷⁾ F.D. BUSNELLI, *Le alternanti sorti del principio di dignità della persona umana*, in *Riv. dir. civ.*, 2019, p. 1071 ss, nel commentare le riflessioni di V. SCALISI, *Ermeneutica della dignità*, Milano, 2018, che attribuisce un valore ermeneutico propulsivo alla dignità, coinvolgendo la sfera esistenziale, sociale e relazionale della persona.

⁽¹⁸⁾ P. RONFANI, *Dal bambino protetto al bambino partecipante. Alcune riflessioni sull'attuazione dei “nuovi” diritti dei minori*, in *Soc. dir.*, 2001, p. 77 ss; A. BUCELLI (a cura di), *Identità e salute del minore. Problematiche attuali*, Pisa, 2021, e in particolare, il contributo di F.D. BUSNELLI, *Immagini vecchie e nuove della tutela della salute del minore*, p. 14 ss., che richiama la necessità di calibrare le istanze di tutela all'evoluzione della persona minore di età, nel rispetto dei principi costituzionali espressi dal combinato disposto di cui agli art. 2 e 31 Cost.

migliorare le “abilità relazionali”, ma anche — e soprattutto — per tutelare la salute psico-fisica dell’utente.

A partire da questi spunti, la trattazione esplora la portata degli obblighi di alfabetizzazione (c.d. *literacy*) ⁽¹⁹⁾ introdotti dal legislatore europeo per fornitori e *deployers* rispetto agli utilizzatori di ciascuna fase di sviluppo e utilizzo di sistemi basati sull’intelligenza artificiale. Ciò al fine di valutarne le più ampie implicazioni sul sistema di responsabilità e sui meccanismi di responsabilizzazione nella società dell’informazione. Infatti, gli obblighi e responsabilità dei prestatori di servizi e produttori, degli esercenti le responsabilità genitoriali, educatori e istituzioni saranno letti in funzione della necessità di individuare soluzioni volte a rendere obbligatoria la trasmissione di conoscenze e strumenti di valutazione per le nuove generazioni, come risposta di politica del diritto volta ad assicurare nell’utilizzo di servizi e prodotti tecnologici la protezione dei dati personali, dell’identità e, più in generale, promuovere il benessere nella dimensione digitale dei giovani utenti.

Per tale ragione, le note vulnerabilità cui è esposto in generale l’utente digitale (come la lotta a comportamenti illeciti volti ad arrecare pregiudizi diretti, ad esempio il *phishing*, ovvero legati alla falsa rappresentazione di persone o eventi, come il furto di identità o condotte di misinformazione e manipolazione, o alla diffusione di *spam* e *malware* o di notizie confidenziali) saranno adattate a scenari comuni per bambini e adolescenti anche nella fruizione dei servizi digitali tra pari. L’attenzione è rivolta anche a forme di dipendenza e abuso rispetto agli strumenti digitali, che viene espressa nell’enunciazione del diritto alla disconnessione. Il che conferma l’importanza della valorizzazione delle relazioni sociali e familiari nella dimensione fisica e reale. Usi impropri, infatti, della permanenza *online* possono facilmente compromettere la salute mentale e la crescita dell’utente minorenni. L’educazione digitale va dunque ad aggiungersi (e non a sostituirsi) a quelle competenze e bagaglio di conoscenze ed esperienze, che sono propri della dimensione fisica, specialmente con riferimento alla sfera emotiva e relazionale.

Una volta identificati i diritti, serve una ferma strategia di attuazione degli stessi, atta non solo ad allocare ruoli e responsabilità al fine di risarcire eventuali danni subiti in caso di compromissione, ma —

(19) Art. 4, Regolamento UE 2024/1689, cit e su cui *infra*, cap. 3.

come osservato — soprattutto a prevenire il verificarsi dei rischi di esposizione dell'utente a pericoli per la propria sicurezza, incolumità e salute attraverso un continuo monitoraggio dell'efficacia dei meccanismi di responsabilizzazione.

Alla luce di tali premesse, procederemo, dunque, all'analisi dei modelli adottati nelle esperienze nazionali e internazionali, facendo emergere che i rischi della dimensione digitale siano in larga misura condivisi anche fuori dai confini dell'Unione Europea. Per tale motivo potremo considerarli una ragionevole base per l'elaborazione di modelli normativi capaci di mitigare il possibile impatto negativo della digitalizzazione sulla crescita e benessere di *tutti* i fanciulli. Noteremo, infatti, come le risposte al livello di politica del diritto possano non adottare gli stessi parametri e sortire effetti diversi sulla società di riferimento, pur condividendo tutte le premesse relative alla necessità e urgenza di intervenire per costruire un ambiente digitale sicuro e rispettoso dei diritti fondamentali dell'infanzia, per addivenire ad incentivare forme di responsabilizzazione dei diversi attori.

4. La metodologia di indagine adottata nel presente volume tende a verificare l'adattabilità alla dimensione digitale delle interpretazioni applicative relative ad alcuni istituti volti a tutelare i diritti fondamentali dei minori di età nelle relazioni fra privati. A tal fine, analizzeremo — in diverse esperienze nazionali appartenenti a più famiglie giuridiche e caratterizzati da un diverso stadio di transizione digitale dei servizi e prodotti — gli approcci dei legislatori rispetto alla costruzione di un ambiente digitale alla portata dei minori di età. Ciò allo scopo di cogliere nelle interpretazioni nazionali elementi comuni che siano coerenti con gli approcci adottati nelle normative di settore volti a mitigare rischi di compromissione di diritti considerati universali, come quelli dei minori di età, anche nella dimensione digitale, fornendo risposte di politica del diritto che siano sufficientemente armonizzate e condivise dagli operatori da poter trovare efficace attuazione al pari degli *standard* tecnici, riconosciuti globalmente ⁽²⁰⁾.

A questo proposito, faremo dunque tesoro delle prassi interpreta-

⁽²⁰⁾ Fonte di ispirazione le parole di Varano nel ricordare il pensiero di Pizzorusso “*Mi pare, in conclusione, che in queste poche righe siano già abbastanza chiari, sia pure in nuce, i punti essenziali del metodo comparativo che ha in mente Pizzorusso: recupero universalità del diritto, rapporto stretto fra scienza e realtà, aspirazione a un approccio unitario della comparazione quale che sia l'area — diritto pubblico o diritto privato — nella quale lo si utilizzi*”, così V. VARANO, in Alessandro Pizzorusso e la

tive raccolte da raccomandazioni, linee guida e pareri delle autorità garanti e organizzazioni di settore che consentano di colmare eventuali lacune e risolvere paradossi emergenti dagli adattamenti applicativi degli istituti di diritto privato a tutela dei minori già sussistenti per gli scenari reali. Ci occuperemo, ad esempio, delle problematiche relative all'incapacità del minore e degli spazi di autonomia che i giovani utenti a seconda delle fasce di età di fatto acquisiscono, esprimendo un consenso valido, come condizione di liceità dei trattamenti di dati personali e alle relative implicazioni di sistema in materia di rappresentanza legale. In questo modo saremo in grado di offrire spunti di riflessione per sviluppare proposte suscettibili di applicazione in più contesti e sistemi giuridici, con l'ambizione di costruire le premesse per un ambiente digitale alla portata dei bambini e degli adolescenti ⁽²¹⁾.

Considerato, poi, che gli avanzamenti dello stato dell'arte tecnologico si misurano attraverso regole di diligenza, *standard* tecnici e certificazioni, dedurremo possibili risvolti sistematici della mancata o parziale aderenza agli stessi in termini di responsabilità e responsabilizzazione. Trattandosi di procedure metodologiche basate su requisiti e condizioni che, se soddisfatti nel caso concreto, validano l'intero processo e i risultati in termini di qualità rispetto agli obiettivi dichiarati, gli *standard* tecnologici possono contribuire, infatti, come norma operativa per misurare il grado di diligenza professionale nel settore di riferimento. Se il fenomeno della datificazione della società è disciplinato sulla base delle risultanze delle valutazioni di impatto condotte di volta in volta dagli attori, l'adesione o meno a una misura di salvaguardia condivisa nella comunità scientifico-tecnologica consente di determinare sul piano giuridico i confini delle condotte responsabilizzate (*rectius* diligenti o *accountable*) al fine di mitigare un rischio noto, richiedendo contestualmente all'attore di giustificarne eventuali discostamenti. Di fatto, seguire lo *standard*, laddove sussistente e riconosciuto, può costituire una presunzione di conformità alla norma da parte del singolo operatore, che abbia adottato quella particolare

comparazione, in *Diritto pubblico comparato ed europeo*, 2017, p. 285 nel commentare il contributo A. PIZZORUSSO, *L'apporto della comparazione alla scienza*, Milano, 1980.

⁽²¹⁾ Sulla circolazione dei modelli, R. SACCO, *Circolazione e mutazione dei modelli giuridici*, in *Dig. disc. priv.*, Sez. civ., v. II, Torino, 1988, 365 ss.

misura tecnica, predeterminando così i livelli di diligenza professionale ⁽²²⁾.

Vedremo dunque come la spontanea adesione, veicolata (o meno) da una forma di auto-regolamentazione degli operatori coinvolti in valutazioni di impatto analoghe, possa risultare particolarmente efficace in termini di *soft law*. In questa prospettiva, infatti, il legislatore europeo incoraggia l'esercizio dell'autonomia privata attraverso l'elaborazione di codici di condotta e certificazioni, quali meccanismi virtuosi promotori di "corrette interpretazioni" ⁽²³⁾ delle norme.

Lo sforzo interdisciplinare volto a coniugare condizioni tecniche con quelle giuridiche corrobora la accennata scelta metodologica di mappare lo stato dell'arte in materia attraverso la raccolta di prassi nazionali e locali, anche extraeuropee. Con l'intento di costituire, infatti, a partire dall'analisi comparatistica delle iniziative in materia di diritti digitali dei minori di età, un banco di prova sistematico orientato a identificare in maniera universale i possibili adattamenti interpretativi che le diverse architetture costituzionali e i valori specifici condivisi in un determinato momento storico richiedono negli scenari concreti. Si pensi, a titolo esemplificativo, che l'analisi dei rischi e delle opportunità offerti dalla singola applicazione potrebbe mutare per ciascuna categoria di utente e dipendere da una serie di variabili legate al contesto socio-economico-educativo che richiederebbero priorità di intervento normativo con contenuti e modalità applicative differenziate. A seconda del livello di digitalizzazione e del grado di transizione digitale dei servizi e dei prodotti, ovvero delle condizioni personali dell'utente (età, educazione, salute, etc.), infatti, la stessa persona può risultare più o meno vulnerabile rispetto a un determinato trattamento di dati, a una certa applicazione digitale o soluzione tecnologica. Di conseguenza, anche la risposta normativa e quella istituzionale devono potersi adattare.

Vedremo, infatti, come la maggior parte delle strategie sulla dati-

⁽²²⁾ L'evoluzione giuridica è data da trapianti e recepimenti che possono essere imposti, ovvero semplicemente acquisiti in quanto considerati scelta economicamente più efficace o per spirito di imitazione verso sistemi considerati più autorevoli "*Thus, 'prestige' motivates imitation*", Così M. GRAZIADEI, *Comparative Law, Transplants, and Receptions*, in M. REIMANN - R. ZIMMERMANN (eds), *The Oxford Handbook of Comparative Law*, 2nd edn, Oxford Handbooks 2019, p. 456 ss.

⁽²³⁾ Così ad es., l'art. 40 del Reg. UE 679/2016, Regolamento generale sulla protezione dei dati personali.

ficazione della società e sull'innovazione sia orientata ad introdurre obblighi sulla base della percezione del rischio di un determinato servizio o prodotto digitale o flusso di dati da parte dell'attore, e che tale meccanismo sia in ogni caso veicolato da una classificazione della società in categorie di soggetti con caratteristiche determinate (*rectius* vulnerabilità) che possono in misura più o meno rilevante esporre il singolo individuo a una maggiore probabilità di occorrenza e a un pregiudizio più o meno grave in termini di serietà ⁽²⁴⁾. Noteremo che la sfida residuale consista dunque nell'investigare (e di conseguenza costruire) metodologie capaci di identificare le vulnerabilità del singolo utente oltre gli elementi noti che possano determinare l'esposizione a rischi propri della dimensione digitale (come l'età e la capacità di discernimento nel nostro caso).

A questo proposito, nel presente contributo ricostruiremo un modello di tutela e promozione dei diritti dell'infanzia e dell'adolescenza a partire dalla lettura in una sorta di matrice complessa delle fonti normative, della giurisprudenza, della letteratura scientifica e dell'insieme delle misure tecniche e organizzative sviluppate in assenza di norme specifiche ed esaustive sul punto. Parimenti valorizzeremo in termini di buone prassi, vuoi per le potenzialità di riproducibilità in diversi sistemi giuridici, vuoi per la replicabilità in una pluralità di scenari applicativi, quegli elementi in grado di facilitare la circolazione delle opportunità, attraverso i servizi e i prodotti della società dell'informazione, in maniera affidabile.

Noteremo che resta aperto, tuttavia, il problema di come analizzare l'impatto sull'utente che rispetto ad una certa applicazione possa risultare mediamente vulnerabile e, per ragioni anche momentanee o personali, diventi per altre applicazioni altamente esposto o, viceversa, digitalmente più consapevole di altri — apparentemente — non vulnerabili.

5. Alla luce dell'illustrazione degli elementi che caratterizzano la transizione digitale dei diritti fondamentali dei minori emerge il contributo delle scienze giuridiche nell'interpretare la tecnica, intesa come insieme di conoscenze che caratterizzano oggi il progresso scientifico e l'innovazione. Integrare le misure di salvaguardia nel ciclo di vita dello sviluppo di un servizio o di un prodotto della società dell'informazione

⁽²⁴⁾ G. COMANDÉ, *Introduction to the Encyclopedia of Law and Data Science: 'Directions for Use'*, in Elgar Encyclopedia of Law and Data Science, 2022, ix ss.

non significa solo conformarsi a una norma, ma interpretare la dimensione digitale riaffermando i valori democratici in quel determinato scenario.

Prendersi cura dello sviluppo psico-fisico e del benessere dei bambini significa dunque proteggerli sì dall'esposizione a pericoli per la sicurezza e l'incolumità, ma anche garantire loro l'accesso paritario alle diverse opportunità offerte dalla società dell'informazione e dall'innovazione tecnologica, definendo un modello di promozione e attuazione capace di circolare e adattarsi alle architetture giuridiche dei diversi sistemi, con la consapevolezza di dover affrontare rischi comuni per diritti considerati universali.

In quest'ottica, la ricostruzione sistematica del quadro normativo attraverso la combinazione dei contributi dei diversi formanti giuridici porta a costruire un modello capace di coniugare i principi informatori della società dell'informazione con i contenuti di cui si riempie la formula dei c.d. interessi superiori dei bambini nella dimensione digitale, in particolare: la responsabilizzazione (*accountability*) degli attori assumerà connotati specifici rispetto alla protezione di minori di età in ragione della loro (in)capacità; la trasparenza, in senso tecnico, rispetto ai processi decisionali automatizzati e in senso organizzativo, relativamente agli obblighi informativi, richiederà tecniche di comunicazione adattate all'utenza minorenni; infine l'equità (*rectius* la *fairness*), volta a perseguire obiettivi di inclusività nell'ambiente digitale, evitando la produzione di effetti discriminatori, sarà articolata in ottica di accesso paritario alle risorse e alle conoscenze, nonché misurata in ottica prognostica rispetto alla naturale evoluzione della persona.

Nel presente contributo l'approfondimento sulla regolamentazione della società dell'informazione e dell'innovazione tecnologica offerto nel primo capitolo diventa più granulare nel secondo, dove si esplorano le modalità di protezione dei diritti fondamentali del fanciullo a fronte della digitalizzazione dei prodotti e dei servizi. Ivi si coglie il ruolo di armonizzazione delle buone prassi intraprese dagli *standard* tecnici elaborati dagli operatori economici; mentre nel terzo capitolo, l'attenzione si sposta verso la promozione degli interessi superiori del fanciullo per una datificazione della società a portata di bambini e adolescenti.

La riflessione sulla categoria dei minori di età consente, infine, di ridisegnare il concetto di vulnerabilità nello spazio digitale, cogliendone le caratteristiche di universalità (rispetto alla metodologia da

applicare per mitigare rischio di pregiudizio all'individuo e al gruppo di persone) e allo stesso tempo di personalizzazione rispetto alla posizione dell'individuo (relativamente al gruppo o ai gruppi di soggetti portatori della medesima vulnerabilità), nonché rispetto al possibile mutamento della condizione del soggetto dovuta a fattori temporali o giuridici o naturali (come il compimento della maggiore età o dell'età sufficiente per un determinato atto, o l'acquisizione di uno *status* civile, o la guarigione da una malattia, etc.) ⁽²⁵⁾.

Come osservato, il metodo comparatistico fornirà un ulteriore supporto alla lettura dei fenomeni sociali al fine di proporre indicazioni operative di politica del diritto, che possano aspirare a costituire un modello capace di circolare nei diversi sistemi giuridici con gli opportuni adattamenti, in modo da indirizzare in maniera quanto più armonizzata possibile le caratteristiche universali del fenomeno della digitalizzazione e il relativo impatto sui bambini. In particolare, misurando “*le differenze che intercorrono tra i diversi sistemi giuridici analizzati*” e controllando “*la coerenza dei vari elementi presenti in ogni sistema*” ⁽²⁶⁾, saranno valorizzati quegli elementi da ricondurre a regole operazionali condivise in più ordinamenti, al fine di ricostruire le possibili condizioni di applicabilità in scenari diversi. Saranno, inoltre, individuate quelle variabili suscettibili di soddisfare in maniera più efficace gli obiettivi di tutela, ma soprattutto di promozione, dei diritti dei minori di età nella dimensione digitale ⁽²⁷⁾, sfruttando altresì il carattere universale dei rischi di compromissione degli stessi e delle contromisure tecniche e tecnologiche che rispondono concretamente ai pericoli.

6. Gli esiti dell'analisi portano infine ad un'ulteriore riflessione,

⁽²⁵⁾ N. HELBERGER, M. SAX, J. STRYCHARZ, H.-W. MICKLITZ, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, in *Journal of Consumer Policy*, 2022, 45:175-200; A. COLE, *All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique*, *Critical Horizons*, 2016, 17(2), 260-277; M. ALBERTSON FINEMAN, *The vulnerable subject: Anchoring equality in the human condition*, in *Yale Journal of Law & Feminism*, 2008, 20, 1 s; L. GATT, *Legal anthropocentrism between nature and technology: the new vulnerability of human beings*, (2022) 1 EJPLT, 15-26. DOI: <https://doi.org/10.57230/EJPLT221LG>.

⁽²⁶⁾ Sulla scia della terza e della quarta tesi di Trento, elaborate da R. SACCO nel 1987, disponibili su <http://www.jus.unitn.it/faculty/guida/tesi.html>.

⁽²⁷⁾ Secondo la logica di identificare *common core* e *better rule*, applicata alle interpretazioni dei quadri normativi che insistono sulla tutela e promozione dei diritti dei minori di età, K. BOELE-WOELKI, *Common Core and Better Law in European Family Law*, Intersentia, 2005.

concernente un ripensamento circa la portata delle attuali declinazioni del concetto di vulnerabilità. Nella società dell'informazione, infatti, un richiamo normativo per definire l'esposizione del soggetto interessato a pericoli derivanti dalla circolazione di informazioni personali può essere individuato nell'art. 9 del Regolamento Europeo n. 2016/679 (Regolamento generale in materia di protezione dei dati personali, di seguito anche "GDPR"), che stabilisce basi giuridiche stringenti per legittimare il trattamento di dati cc.dd. appartenenti a particolari categorie. Questi ultimi espongono, per l'appunto, il soggetto interessato a pericoli derivanti dalla classificazione dell'individuo in un gruppo riconducibile ad una possibile minoranza e, pertanto, la rendono suscettibile di essere vittima di discriminazioni per tale particolare caratteristica. È per questa ragione che si impongono misure di salvaguardia per poter abilitare detta tipologia di flussi di dati, che altrimenti potrebbero essere facilmente suscettibili di improprio e malevolo utilizzo. Non è un caso che le categorie di dati cc.dd. sensibili corrispondano ai fattori di rischio discriminatorio ai sensi delle Direttive Europee del 2000 ⁽²⁸⁾, a cui si sono aggiunte le informazioni di carattere sanitario, genetico e biometrico.

In primo luogo, le vulnerabilità note nella dimensione fisica non sempre trovano univoca corrispondenza nella dimensione digitale, che a sua volta fa emergere assieme all'esposizione a nuovi rischi, vulnerabilità proprie. L'analisi dei rischi emergenti dalla digitalizzazione dei servizi e dei prodotti, porta a ripensare a come declinare le vulnerabilità in ogni settore economico, anche in ragione delle tipologie di mezzi e delle diverse finalità dei trattamenti. L'avvento dell'intelligenza artificiale, intesa come "famiglie di tecnologie" ⁽²⁹⁾, impone di adottare un approccio dal basso, basato di volta in volta a identificare i rapporti di asimmetria di potere da controbilanciare con gli istituti di diritto privato disponibili. Si pensi all'impatto della datificazione nei rapporti di lavoro, ove la transizione digitale dei processi ha ridisegnato (e ridisegna) anche l'oggetto, i mezzi, gli spazi e il tempo della prestazione lavorativa e, non solo le modalità di comunicazione: dal telelavoro,

⁽²⁸⁾ Direttiva 2000/43/CE del Consiglio, del 29 giugno 2000, che attua il principio della parità di trattamento fra le persone indipendentemente dalla razza e dall'origine etnica e Direttiva 2000/78/CE del Consiglio, del 27 novembre 2000, che stabilisce un quadro generale per la parità di trattamento in materia di occupazione e di condizioni di lavoro.

⁽²⁹⁾ Così il menzionato Regolamento UE n. 1689/2024.

all'introduzione di macchine intelligenti a supporto di attività ripetitive di tipo industriale o commerciale, ma anche amministrativo-organizzativo, come nelle procedure di reclutamento, gestione della carriera e valutazione delle *performance* dei lavoratori. Del pari, in ambito sanitario, ove l'innovazione tecnologica si inserisce nelle dinamiche dei rapporti di cura tra medico e paziente, si rendono necessari nuovi bilanciamenti, sia per adempiere agli obblighi previsti dalla normativa di settore, sia per conformarsi ai principi informativi della materia, che a loro volta si arricchiscono di nuovi contenuti interpretativi per gli adattamenti necessari per la tenuta del sistema di ruoli e responsabilità nella dimensione digitale ⁽³⁰⁾: anche in questo caso dalla telemedicina, alla medicina personalizzata, ai supporti robotici o di realtà virtuale nelle attività di diagnosi, trattamento e riabilitazione.

In secondo luogo, nell'eseguire le diverse valutazioni sugli impatti che determinate soluzioni tecnologiche producono sulla persona utente e sui relativi di diritti fondamentali, occorre prendere in considerazione le opportunità offerte dalla società dell'informazione e le relative implicazioni sulla definizione stessa di vulnerabilità: nel caso oggetto di analisi nel presente contributo, la sfida è di identificare di quali nuovi contenuti si possa riempire la formula degli interessi superiori del fanciullo nella dimensione digitale, ciò non solo per costruire un sistema di tutele efficace, ma soprattutto per promuovere una società dell'informazione a portata di bambini e adolescenti. Già la normativa a tutela del consumatore aveva invero posto l'attenzione sulla necessità di distinguere le forme di tutela per i prodotti destinati a bambini di fasce di età diverse ⁽³¹⁾. Lo stesso art. 8 GDPR affronta la questione dell'età del soggetto minorenne, operando un bilanciamento volto ad estendere all'infraquattordicenne e — laddove previsto da una norma nazionale, anche all'infraquattordicenne e oltre — la facoltà di esprimere

⁽³⁰⁾ Si vedano i contributi raccolti in Vv.Aa., C. CREA A. DE FRANCESCHI (Eds), *The New Shapes of Digital Vulnerability in European Private Law*, Nomos, 2024.

⁽³¹⁾ Si pensi alla Direttiva UE n. 2009/48/CE sulla sicurezza dei giocattoli per i “prodotti progettati e destinati, in modo esclusivo o meno, a essere utilizzati per fini di gioco da bambini di età inferiore ai 14 anni”, oppure alla Direttiva UE n. 2005/29/CE sulle pratiche commerciali scorrette che si preoccupa di introdurre il parametro del “punto di vista del membro medio”, da determinarsi in via interpretativa rispetto alle possibili reazioni tipiche di fronte a una sollecitazione, per valutare l'impatto di una pratica rivolta a un gruppo di soggetti vulnerabili, citando il caso dei bambini. Sul punto, G. HOWELLS, H.W. MICKLITZ, T. WILHELMSSON, *European Fair Trading Law. The Unfair Commercial Practices Directive*, London, 2006.

autonomamente un consenso valido per autorizzare il trattamento dei propri dati personali processati nell'ambito di servizi digitali. A questo proposito, analizzeremo le iniziative regolatorie volte a valorizzare l'autonomia decisionale degli adolescenti nella dimensione digitale, rispetto ad un bilanciamento maggiormente orientato alla rappresentanza del genitore riservato ai bambini, anche al fine di consentire una risposta interpretativa aderente alla realtà che vede un utilizzo quotidiano da parte di bambini e adolescenti di strumenti digitali.

Identificare i requisiti giuridici, le condizioni tecniche e le implicazioni di politica del diritto per promuovere un paradigma condiviso di protezione e promozione dei diritti dell'infanzia e dell'adolescenza nella dimensione digitale, affinché quest'ultima sia accessibile in maniera sicura e affidabile a tutti, costituisce l'obiettivo primario della presente trattazione. Parallelamente ci si propone di raggiungere un'altra evidenza: ovvero contribuire a delineare come la società dell'informazione abbia messo in crisi il concetto stesso di vulnerabilità.

Da un lato, infatti, osserveremo come rischi e opportunità dei servizi e prodotti digitali contribuiscano a disegnare i contenuti e i confini degli interessi superiori dei minori nella società attuale. Attraverso l'identificazione di misure tecnico-organizzative volte a prevenirne la compromissione e mitigarne gli effetti pregiudizievoli, elaboreremo gli adattamenti dei paradigmi di *accountability* definiti per gli adulti alle specifiche vulnerabilità da tutelare e alle opportunità da cogliere per gli utenti minori di età. Dall'altro lato, tuttavia, osserveremo come dalla mappatura delle possibili declinazioni degli interessi superiori dei minori di età nella dimensione digitale sia possibile cogliere quelle opportunità "irrinunciabili", che la dimensione digitale offre ai giovani utenti per avviarli ad una consapevole costruzione della società del domani. Nello sviluppo del ragionamento, il riferimento alle vulnerabilità multiple del minore di età costituirà, così, l'occasione per corroborare il sistema e validare le proposte operative cui addiverremo.

Analizzeremo, ad esempio, come la visione umano-centrica espressa dalle normative di settore portino a valorizzare l'importanza di una progressiva — ma effettiva — partecipazione anche degli utenti minorenni ai processi di co-creazione di buone prassi e validazione dei sistemi. Il concetto di vulnerabilità ne uscirà, dunque, come categoria fluida rispetto al singolo e alla comunità di riferimento, strumentale all'identificazione dei limiti di azione al fine di riaffermare i valori di inclusività e democrazia in uno spazio globale e in un tempo in(de)fi-

nito, come quello digitale che per essere alla portata dei minori di età, deve poter essere costruito con il loro contributo.

Di conseguenza ci porremo l'interrogativo in ordine all'attualità delle odierne categorie giuridiche volte a proteggere il (patrimonio del) minore di età rispetto ad una acquisizione progressiva di strumenti e abilità capaci di ridisegnare i confini dell'incapacità del minore di età, distinguendo forme diversificate di autonomia decisionale e operativa — soprattutto derivante dall'uso quotidiano dei servizi e dei prodotti della società dell'informazione.

In questo contesto, come terzo e ultimo obiettivo del contributo, proporremo una valorizzazione — mediante l'individuazione di percorsi formativi certificabili — del principio di alfabetizzazione rispetto alla digitalizzazione e ai sistemi di intelligenza artificiale come requisito, in presenza di determinate condizioni, per consentire agli esercenti le responsabilità genitoriali, agli educatori, agli operatori economici di volta in volta di valutare — secondo il proprio ruolo e le proprie responsabilità — l'effettiva acquisizione di un determinato livello di capacità di discernimento che sia considerato sufficiente ad accordare spazi ai giovani utenti per agire progressivamente in misura più indipendente e perseguire i propri interessi in maniera più indipendente.

CAPITOLO I

DATIFICAZIONE DELLA SOCIETÀ E NUOVE TECNOLOGIE: LEGGERE IL QUADRO REGOLATORIO ATTRAVERSO LE LENTI DEI MINORI DI ETÀ

SOMMARIO: 1. Il quadro regolatorio: governare la dimensione digitale e le nuove tecnologie tra rischi e opportunità. — 2. Il Regolamento europeo sulla protezione dei dati personali e la questione relativa all'età per esprimere un valido consenso. — 2.1. I minori di età, la protezione dei dati e il caso Open AI. — 3. Gratuità e affidabilità: quali strumenti di tutela per gli utenti inconsapevoli? — 4. Il Regolamento europeo sui servizi digitali: gli obblighi di trasparenza. — 4.1. (*Segue*). Gli obblighi di protezione per i minori di età. — 5. Le ricadute su specifiche normative di settore: il Regolamento sui mercati digitali (DMA). — 5.1. (*Segue*). La regolamentazione dei contenuti audiovisivi. — 6. (*Segue*). Il dibattito sulla regolamentazione dei neurodiritti. — 7. La regolamentazione UE per lo sviluppo di sistemi IA affidabili. — 7.1. (*Segue*). L'intelligenza artificiale a portata dei minori di età: i lavori dell'UE e del Consiglio d'Europa a partire dalle raccomandazioni elaborate dall'UNICEF. — 8. La regolamentazione della società dei dati nei sistemi extra-UE. — 8.1. I sistemi di *Common Law*. — 8.2. Il *Digital Charter Implementation Act* canadese e il Codice civile del Québec. — 8.3. L'approccio negli USA e le iniziative statali: cenni. — 9. I sistemi tecnologicamente avanzati in Asia e Oceano Pacifico. — 9.1. La tutela dei dati personali "adeguata" in Corea del Sud e Giappone e i relativi approcci verso i minori di età. — 9.2. Il sistema cinese: cenni e rinvio. — 9.3. Il *Digital Personal Data Protection* indiano. — 10. Le strategie a portata di bambini e adolescenti nei sistemi sudamericani. — 10.1. (*Segue*). Perù. — 10.2. (*Segue*). Argentina. — 10.3. (*Segue*). Il sistema di tutele in Brasile e la risoluzione "settoriale": cenni e rinvio. — 11. I sistemi africani: cenni alle misure introdotte in Swaziland, Uganda e Ruanda. — 12. Regolamentare la società dell'informazione e le nuove tecnologie per i minori di età: osservazioni di sintesi.

1. Il quadro regolatorio: governare la dimensione digitale e le nuove tecnologie tra rischi e opportunità.

La digitalizzazione delle informazioni ha aperto una nuova dimensione per interpretare le relazioni tra privati: dalla comunicazione fra persone, ai trasferimenti di capitali, alla transizione digitale di servizi e

prodotti, la quotidianità è oggi caratterizzata dalla presenza preponderante della tecnologia ⁽¹⁾.

L'accelerazione di questo fenomeno è dovuta non solo al progressivo avanzamento degli strumenti tecnologici, sempre più sofisticati e allo stesso tempo accessibili sul mercato, ma anche al nuovo modo di concepire la digitalizzazione, come dimensione alternativa a quella fisica, capace spesso di far superare le fragilità, i limiti e di costruire nuovi equilibri, ma anche di esporre le persone a nuove vulnerabilità note (e non). Si pensi, ad esempio, al periodo pandemico quando le relazioni personali, contrattuali, lavorative sono state esercitate prevalentemente “da remoto” ⁽²⁾. In tale occasione, anche al fine di mantenere livelli accettabili (se non più efficaci) di produzione e *performance* — quanto meno in alcuni settori — una repentina transizione digitale dei processi ha portato ad instaurare rapidamente nuovi equilibri socio-economici e a ripensare alla declinazione dei diritti fondamentali della persona con l'urgenza di un intervento sia nei servizi pubblici, che nelle attività private, per la regolamentazione dei rapporti fra consociati e tecnologie e tra consociati mediante le tecnologie ⁽³⁾.

Governare la dimensione digitale significa, in primo luogo, comprenderne la portata innovativa rispetto alla realizzazione della persona umana, come singolo e come appartenente ad una comunità. In secondo luogo, indica la necessità di stabilire investimenti e allo stesso tempo paradigmi di responsabilità comuni capaci di adattarsi alle vulnerabilità da proteggere e agli interessi da promuovere caso per caso.

Parlare di “opportunità e rischi” ⁽⁴⁾ nel contesto digitale significa

⁽¹⁾ A. SESTINO, A. KAHLAWI, A. DE MAURO, *Decoding the data economy: a literature review of its impact on business society and digital transformation*, in *European Journal of Innovation Management*, 2023, doi: <https://www.emerald.com/insight/content/doi/10.1108/EJIM-01-2023-0078/full/html>; V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: a revolution that will transform how we live, work, and think*, Mariner Books, New York, 2014.

⁽²⁾ D.P.C.M., 4 marzo 2020, Ulteriori disposizioni attuative del decreto-legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, applicabili sull'intero territorio nazionale.

⁽³⁾ EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *The coronavirus pandemic and fundamental rights: A year in review*, 2021, doi:10.2811/68877.

⁽⁴⁾ La formula, nata nell'ambito degli *standard* sviluppati in materia della gestione dei rischi aziendali, confluita nella norma ISO 9001:2005, trova spesso

invitare gli operatori del diritto a adottare un processo di co-creazione ⁽⁵⁾ delle politiche del diritto assieme ai diversi portatori di interessi (dalle aziende, ai cittadini, ai rappresentanti dell'associazionismo, ai servizi pubblici etc.). Ciò affinché nessun settore e nessun applicativo restino esclusi da una valutazione di merito, che porti ad abilitare una determinata soluzione, in ragione dell'implementazione di misure volte a mitigare il pericolo di arrecare danno al singolo (o alla comunità) che siano considerate efficaci al punto da poter concludere di cogliere la sfida digitale, godere dei benefici dell'operazione/processo/sistema proposto. L'adozione di questo approccio, tuttavia, appare efficace solo laddove l'analisi non sia limitata ad una prospettiva umano-centrica rivolta all'interessato che corrisponde all'utente medio, ma vada a incidere positivamente sui livelli di inclusività, evitando discriminazioni e implicazioni negative sui diritti della persona.

Per tale ragione appare particolarmente rilevante leggere i testi normativi con le lenti dei soggetti deboli della società che, non solo non devono essere esclusi dal bersaglio della valutazione delle soluzioni della rivoluzione digitale, ma devono poter agire come parte attiva dei processi di co-creazione di nuove politiche di diritto per promuovere i loro interessi rispetto alle nuove frontiere tecnologiche.

In particolare, in questo capitolo analizzeremo gli approcci regolatori alla dimensione digitale, concentrandoci sugli aspetti dedicati alla tutela dei minori di età. Ciò non solo al fine di ricostruire una tassonomia dei rischi specifici identificati nelle diverse iniziative legislative come foriere di pregiudizio allo sviluppo psicofisico di utenti non adulti (in modo da misurarne la portata e trarne indicazioni di politica del diritto per un ambiente digitale e soluzioni tecnologiche a

applicazione nelle procedure di conformità agli obblighi formulati per la gestione dei flussi informativi nella transizione digitale dei servizi e dei prodotti che caratterizza la datificazione della società, è ripresa nel considerando 56 del Regolamento sull'IA, in materia di alfabetizzazione.

⁽⁵⁾ Anche le metodologie di co-creazione nascono dall'esperienza di analisi di gestione del rischio aziendale a partire dalle esperienze dei consumatori, si vedano C. GENTILE, N. SPILLER, G. NOCI, *How to Sustain the Customer Experience: An Overview of Experience Components that Co-create Value With the Customer*, *European Management Journal*, Volume 25, Issue 5, 2007, pp. 395 ss., C.K. PRAHALAD, VENKAT RAMASWAMY, *Co-creation experiences: The next practice in value creation*, in *Journal of Interactive Marketing*, Volume 18, Issue 3, 2004, pp. 5 ss., G. RITZER - N. JURGENSON (2010), *Production, Consumption, Prosumption: The nature of capitalism in the age of the digital 'prosumer'*, *Journal of Consumer Culture*, 10(1), 13.

misura di bambini); ma anche al fine di tracciare una mappatura delle opportunità (note e meno note) offerte ai giovanissimi utenti dalla società dell'informazione, capaci — invero — di personalizzare le esperienze di crescita e maturazione del singolo, abbattendo barriere che, altrimenti, nella dimensione fisica, fungerebbero da ostacolo all'accesso a pari opportunità.

Con metodo comparativo ⁽⁶⁾, le iniziative legislative dell'UE in materia di dati e innovazione tecnologica saranno analizzate e confrontate con altre esperienze, anche extra europee, al fine di far emergere possibili paradossi e soprattutto buone prassi, rispettivamente da riportare a sistema e da sostenere, al livello transnazionale e intersettoriale, trattandosi di sfide che coinvolgono non solo l'UE e i propri valori, ma la società civile globale ⁽⁷⁾. L'analisi fornisce, infine, l'occasione per interpretare gli istituti di diritto privato coinvolti nell'interpretazione e attuazione delle nuove norme in ottica comparata ⁽⁸⁾.

2. Il Regolamento europeo sulla protezione dei dati personali e la questione relativa all'età per esprimere un valido consenso.

La prima normativa dell'Unione Europea che presta attenzione alla necessità di coniugare la protezione dei minori di età nella società dell'informazione è il Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali (di seguito anche "GDPR").

L'iniziativa si ispira a una serie di principi volti, da un lato, a introdurre meccanismi di allocazione di ruoli e responsabilità tra gli operatori della datificazione della società e, dall'altro, a richiedere l'attuazione di misure di mitigazione dei pericoli identificati prima dell'attivazione di un determinato flusso di dati. L'approccio basato

⁽⁶⁾ R. SACCO, *Che cos'è il diritto comparato*, Milano, 1992, G. GORLA, *Diritto comparato e diritto comune europeo*, Milano, 1981.

⁽⁷⁾ S. CALZATI, B. VAN LOENEN, *Beyond federated data: a data commoning proposition for the EU's citizen-centric digital strategy*, in *AI & Society*, 2023, <https://doi.org/10.1007/s00146-023-01743-9>, G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022; L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

⁽⁸⁾ Vedremo come la società dell'informazione metta in crisi gli istituti giuridici legati all'incapacità del minore di età e allo stesso tempo richieda, sulla base del principio di precauzione, l'introduzione di nuove forme di tutela da distribuire tra istituzioni e operatori economici, *infra* Cap. 3.

sulla valutazione del rischio attua, in particolare, il principio di *privacy-by-design* e *privacy-by-default* ⁽⁹⁾, anticipando la tutela verso i soggetti interessati — *i.e.* coloro dei cui dati il flusso tratta — affinché siano limitate le conseguenze dannose di una eventuale violazione e, al contempo, la violazione stessa ricada in una percezione in termini di occorrenza, gravità e serietà considerata — caso per caso — accettabile da coloro che, determinando i mezzi e le finalità del trattamento, rispondono dell'operato (*i.e.* i titolari del trattamento) ⁽¹⁰⁾.

Orbene, in questo quadro metodologico — in cui misure tecniche e misure organizzative fungono da pesi e contrappesi rispetto alla necessità di proteggere i dati in termini di disponibilità, integrità e confidenzialità, e alla altrettanto primaria esigenza di garantire la libera circolazione delle informazioni una volta attivati i flussi — il GDPR si scontra con la definizione stessa di minore di età ⁽¹¹⁾.

Infatti, consapevole della quotidianità dell'uso di servizi della società dell'informazione da parte di ragazze e ragazzi, il legislatore europeo ha — da un lato — abbassato la soglia per manifestare un libero, informato e inequivocabile consenso valido ai fini del trattamento dei dati personali dei minori di età al compimento di anni sedici.

⁽⁹⁾ A. CAVOUKIAN, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian*, Ph.D. IDIS 3, 247-251 (2010). <https://doi.org/10.1007/s12394-010-0062-y>, A. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in *Contratto e impresa/Europa*, 2015, p. 197.

⁽¹⁰⁾ G. COMANDÉ - G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali*, IlSole24ore, 2018; M.G. AUTORINO STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e dir. priv.*, 2016, p. 1249; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 2018, p. 106; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2016.

⁽¹¹⁾ La normativa europea non definisce il minore di età, ma mutua la nozione introdotta con la Convenzione ONU sui diritti dell'infanzia e dell'adolescenza (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. La dottrina ha da sempre assunto un atteggiamento critico rispetto alla rigidità del dato formale dell'età per determinare i confini dell'incapacità del minore, si veda ad es. P. STANZIONE, *Capacità (dir. priv.)*, in *Enc. giur.*, V, Roma, 1988, 10, Id., *Capacità e minore età nella problematica della persona umana*, Camerino-Napoli, 1975; C.M. BIANCA, *Diritto civile*, 1, *La norma, i soggetti*, Milano, 1978, 214, in cui già si esprimeva la necessità di "ridimensionare la portata dell'incapacità negoziale del minore, il quale, compatibilmente con l'esigenza della sua protezione, deve poter godere dell'autonomia necessaria per svolgere la sua personalità".

Dall'altro, ha lasciato ai legislatori degli Stati Membri la possibilità di ulteriormente disciplinare la materia, consentendo l'introduzione di una soglia di età diversa, stabilendo, altresì, come limite minimo, il compimento di anni tredici. Molti degli Stati Membri, nel dare attuazione alla nuova normativa in materia di protezione dei dati personali a modifica e abrogazione delle norme previgenti, hanno approfittato per disciplinare la soglia d'età minima necessaria, ma sufficiente, per esprimere il consenso in ordine al trattamento dei dati personali per “*l'offerta diretta di servizi della società dell'informazione ai minori*”, frammentando — di fatto — le prassi all'interno dell'UE ⁽¹²⁾.

Le ricadute di questa strategia regolatoria hanno impattato su diversi profili sul piano della percezione del rischio, sull'interpretazione del principio espresso dall'art. 8 GDPR, soprattutto in una società, come quella attuale, caratterizzata dall'uso e riuso delle informazioni personali al fine di alimentare e migliorare la produzione di beni e l'erogazione di servizi in ogni settore economico ⁽¹³⁾.

In primo luogo, quindi, lo sforzo del regolamento volto ad armonizzare le attuazioni nazionali si vanifica laddove siano offerti livelli di autonomia differenziati a una porzione rilevante degli utenti digitali: secondo le statistiche, infatti, i minori di età compresa tra 11 e 16 anni costituiscono più di un terzo degli utenti ⁽¹⁴⁾. Pertanto, il fatto che il bambino in Italia possa esprimere valido consenso ai sensi dell'art. 2-*quinquies* del d.lgs. n. 196/2003, così come modificato dalla l. n. 101/2018 all'età di anni quattordici e l'omologo francese debba atten-

⁽¹²⁾ F. RESTA, *Consenso del minore in relazione ai servizi della società dell'informazione*, *Commentario al Codice della Privacy*, R. SCIAUDONE (a cura di), Pacini Giuridica, 2023; F.D. BUSNELLI, *Capacità ed incapacità di agire del minore*, in *Dir. fam.*, 1982, p. 61 ss.; F. GIARDINA, *La condizione giuridica del minore*, Napoli, 1984; G. PALMERI, *Diritti senza poteri. La condizione giuridica dei minori*, Napoli, 1994; L. TAFARO, *L'età per l'attività*, Napoli, 2003, p. 36 ss.; G. ALPA, *I contratti del minore. Appunti di diritto comparato*, in *I Contratti*, 2004, p. 520 ss.; M. CINQUE, *Il minore contraente. Contesti e limiti della capacità*, Padova, 2007; G. CAPILLI, *La capacità negoziale dei minori. Analisi comparata e prospettive di riforma*, Torino, 2012, p. 12 ss.; N. IRTI, *Significato giuridico dell'effettività*, Napoli, 2009, p. 13 ss.

⁽¹³⁾ S. VAN DER HOF - E. LIEVENS, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR* (2018) 23, *Communications Law* 33.

⁽¹⁴⁾ EUROSTAT, *Statistics Explained*, Young People - Digital World, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Young_people_-_digital_world.

dere un anno in più ⁽¹⁵⁾ crea delle fratture interpretative che esprimono, di poi, un mancato assetto unitario dell'UE rispetto alla protezione di una categoria di soggetti vulnerabili ⁽¹⁶⁾ con conseguenti problemi operativi e costi da frammentazione per gli operatori di settore.

In secondo luogo, la circoscritta applicazione dell'art. 8 GDPR complica ulteriormente la prospettiva armonizzante, in quanto i servizi digitali non necessariamente sono diretti esclusivamente ad un'utenza minore di età. Pertanto, laddove un servizio digitale sia diretto generalmente agli adulti, ma di fatto sia utilizzato in larga misura da utenti minorenni, occorre definire quale sia l'età minima affinché l'utente possa esprimere un valido consenso al trattamento dei relativi dati personali. Si potrebbe propendere per la maggiore età, facendo perno sulle implicazioni nella sfera contrattuale del soggetto, ovvero privilegiare il regime introdotto dall'art. 8 GDPR, per analogia supportata dalla considerazione che la capacità di discernimento richiesta possa essere sufficientemente matura a sedici anni (ovvero all'età prevista dalla soglia individuata dal legislatore nazionale) anche per prendere posizione sul trattamento dei dati personali, attività da considerarsi in prima battuta ancillare all'erogazione del servizio ⁽¹⁷⁾.

La questione, tuttavia, merita un approfondimento alla luce degli istituti di diritto privato che si pongono in tensione con l'approccio del legislatore europeo.

Occorre, dunque, distinguere le dimensioni del consenso: quello valido ai fini del trattamento dei dati personali e quello espresso verso termini e condizioni d'uso del servizio digitale, che invero coinvolge un profilo ulteriore di indagine: quello relativo alla capacità di agire nella dimensione digitale con o senza l'intervento del rappresentante legale.

Se nella dimensione fisica il minore di età può acquistare oggetti di uso quotidiano (piccole commesse, libri, etc.) in quanto si presume che

⁽¹⁵⁾ EU Commission - Directorate - General for Justice and Consumers, Unit C.3 Data Protection, *Report on the implementation of specific provisions of Regulation (EU) 2016/679*, <https://www.dataguidance.com/sites/default/files/1609930170392.pdf>.

⁽¹⁶⁾ Sia concesso rinviare a D. AMRAM, *Children (in the digital environment)*, in G. COMANDÉ (a cura di), *Encyclopedia of law and data science*, cit., 155 ss.

⁽¹⁷⁾ A MANTELERO, *Children Online and the Future EU Data Protection Framework: Empirical Evidences and Legal Analysis* (2016) 2 International Journal of Technology Policy and Law pp. 169-81 e S. VAN DER HOF, *I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World* (2017) 34(2) Wisconsin International Law Journal, p. 409 s.

siano atti giuridici posti in essere in nome e per conto del legale rappresentante e che, laddove eccepito, siano annullabili; nella dimensione digitale, ove le attività sono tracciate (dall'apertura del profilo, all'accettazione dei termini e condizioni dei servizi, alla navigazione stessa sulla piattaforma) occorrono dei sistemi di verifica *ad hoc* affinché possa operare la *fictio iuris* della rappresentanza ai sensi dell'art. 1389 c.c. italiano ⁽¹⁸⁾. La valutazione — necessariamente da operarsi caso per caso — riguarda, infatti, la clausola di salvaguardia volta a evitare pregiudizi al minore di età per gli atti giuridici posti in essere o ricevuti, i cui effetti possono essere favorevoli o sfavorevoli e determinare, dunque, la validità o meno degli stessi. Per tale ragione, come confermato in giurisprudenza “*debbono considerarsi preclusi al minore atti che importino la perdita di un diritto o l'assunzione di obblighi od oneri*” ⁽¹⁹⁾, ovvero gli stessi devono ricadere necessariamente nella sfera giuridica dei legali rappresentanti.

Le ricadute pratiche dell'asimmetria tra l'impianto dell'art. 2 c.c., letto in combinato disposto con l'art. 316 c.c. e l'art. 2 *quinquies* del Codice in materia di protezione dei dati personali, potrebbero trovare ricomposizione considerando quest'ultimo *lex specialis* capace di abilitare — al pari della legislazione giuslavoristica ⁽²⁰⁾ o di quella sul diritto d'autore ⁽²¹⁾ — il minore a disporre di diritti e obblighi. Infatti, nel caso di superamento della soglia prevista dalla legge sulla protezione dei dati personali, la presunzione di capacità di discernimento su tale profilo potrebbe escludere l'annullabilità del contratto da parte dei legali rappresentanti ai sensi dell'art. 1425 c.c., salvo dimostrare una effettiva incapacità naturale di agire, anche momentanea, dovuta a fattori estranei all'età del minore ⁽²²⁾.

⁽¹⁸⁾ M. CINQUE, *Il minore contraente. Contesti e limiti della capacità*, cit., R. GIARDA, J. LIOTTA, G. RINDI, *Vita quotidiana del minore online. Tra esigenze di tutela e limiti tecnologici*, MediaLaws, 183 ss., E. TOSI, *Contenuti digitali e nuovi consumi: riflessi giuridici dell'innovazione tecnologica sul diritto dei contratti e della responsabilità civile*, in Id. (a cura di), *La tutela dei consumatori in Internet e nel commercio elettronico*, Milano, 2012; M.P. PIGNALOSA, *Contratti a distanza e recesso del consumatore*, Milano, 2016, 253 ss. R. SENIGAGLIA, *Minore età e contratto*, Torino, 2021.

⁽¹⁹⁾ Cass., ord. 13 ottobre 2017, n. 24077, *Foro it.*, I, 2018, 604 ss., con nota di S. STEFANELLI.

⁽²⁰⁾ Art. 1, comma 622, l. n. 296/2006.

⁽²¹⁾ Art. 108, l. n. 633 del 1941.

⁽²²⁾ In tal caso, l'art. 428 c.c. richiede ai fini dell'annullabilità del contratto la malafede del contraente ovvero la sussistenza di un grave pregiudizio nella sfera

Un'ulteriore riflessione riguarda la capacità di comprendere — laddove si presuma quella di discernimento per il trattamento dei dati personali — i rischi propri della dimensione digitale e le implicazioni pregiudizievoli che non necessariamente siano collegate alla sfera patrimoniale del minore. In altri termini, l'attivazione di un profilo su una piattaforma digitale può ben essere a titolo gratuito, in quanto sono i meccanismi di profilazione che determinano il profitto per quel mercato di riferimento e, pertanto, non costituire un'operazione pregiudizievole sotto il profilo economico ⁽²³⁾.

La mancata percezione della contropartita negoziale, tuttavia, può rendere il minore, al pari di qualsiasi altro utente, vulnerabile rispetto all'uso e ri-uso che viene fatto del proprio dato personale. Il rischio di pregiudizio va oltre la sfera patrimoniale. Si arriva, pertanto, a mettere in discussione la premessa sul rapporto tra attività principale e quella ancillare laddove appaia maggiormente rischiosa l'attività di trattamento di dati personali necessaria all'erogazione di un determinato servizio *online*: se l'attività che impatta maggiormente sulla sfera dell'utente è quella collegata alla protezione delle informazioni conferite e/o generate nella dimensione digitale e, al fine di esprimere un consenso valido, il legislatore europeo o nazionale presume la sussistenza della capacità di discernimento nell'infrasedicenne o addirittura nell'infracquattoridicenne, si ribalta — di fatto — il rapporto in termini di rischi derivanti dall'imputazione e disposizione di diritti e obblighi tra attività principale (l'adesione a un servizio digitale) e quella ancillare (il trattamento dei dati personali), soprattutto laddove si resti nella (ampia) area dei servizi digitali disponibili a titolo gratuito ⁽²⁴⁾.

Calando dunque lo scenario nel sistema di tutele approntato dal codice civile, volto per lo più a proteggere la sfera economica del

economica dell'incapace naturale, si veda Cass. 30 settembre 2015, n. 19458. P. RESCIGNO, *Incapacità naturale e adempimento*, Napoli, 1982 e A. QUERCI, *L'incapacità naturale all'esame della giurisprudenza: un contrasto fra massime?*, in *Contratto e impresa*, 2012, p. 1466 ss.

⁽²³⁾ D. KER-E. MAZZINI (2020), *Perspectives on the value of data and data flows*, OECD Digital Economy Papers, No. 299, OECD Publishing, Paris, <https://doi.org/10.1787/a2216bc1-en>.

⁽²⁴⁾ R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, cit.; F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in *Dir. informazione e dell'informatica*, 2018, p. 27 ss. Più in generale sul consenso: G. MARINI, *Il consenso*, in *Trattato di biodiritto*, diretto da S. Rodotà e P. Zatti, *Ambito e fonti del biodiritto*, Milano, 2010, p. 361 ss.

minore di età, occorre procedere ad un accomodamento: se l'utente adolescente, infatti, è considerato sufficientemente maturo per comprendere i ben più gravi rischi derivanti dal trattamento dei dati personali nell'ambito di servizi offerti dalla società dell'informazione, difficilmente si potrà sostenere che non sia capace di discernere anche i vincoli derivanti dall'accettazione di termini e condizioni d'uso dei medesimi servizi. Ciò laddove non siano rinvenibili diverse implicazioni pregiudizievoli nella sfera dell'utente rispetto a quelle che potrebbero derivare dall'uso e riuso dei dati personali da parte del titolare del trattamento.

2.1. *I minori di età, la protezione dei dati e il caso Open AI.*

La rilevanza della questione collegata all'età valida per esprimere il consenso dell'utente per i servizi della società dell'informazione è stata affrontata dall'Autorità Garante per la protezione dei dati personali italiana nell'istruttoria aperta nei confronti della società Open AI LLC, a pochi mesi dal lancio della piattaforma gratuita ChatGPT ⁽²⁵⁾.

Con provvedimento del 30 marzo 2023, il Garante italiano ha imposto una limitazione temporanea in Italia dei servizi erogati dalla piattaforma ChatGPT, incluso il divieto di trattamento di dati personali, ai sensi dell'articolo 58, § 2, *sub f*) GDPR. Numerosi profili di criticità, infatti, erano stati rilevati rispetto alla protezione dei diritti fondamentali degli utenti, specie se minori di età ⁽²⁶⁾.

In particolare, sulla base dei principi di *accountability* e trasparenza, la piattaforma difettava di misure tecniche e organizzative necessarie per accertare l'età degli utenti (in modo da non violare l'art.

⁽²⁵⁾ Sia concesso rinviare al *focus* tematico D. AMRAM (a cura di), *Governo dei dati, Open AI, e salute*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2023, p. 293 ss.

⁽²⁶⁾ AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, provvedimento del 30 marzo 2023, disponibile <https://www.garanteprivacy.it/garante/doc.jsp?ID=9870832>. Nel provvedimento di limitazione, l'Autorità garante ha rilevato l'assenza di un'informativa sulla *privacy* che illustrasse agli utenti e agli interessati come OpenAI LLC avrebbe raccolto ed elaborato i dati nell'ambito di operatività della piattaforma. Inoltre, sono state rilevate altre due lacune rispetto, da un lato, alla condizione di liceità per il trattamento dei dati personali a fini di addestramento degli algoritmi del sistema; dall'altro lato, rispetto ai meccanismi in grado di valutare l'età degli utenti al fine di evitare che infratredicenni utilizzassero il *software*, come invero dichiarato nei termini e condizioni d'uso, che — anche per tale ragione — sono state ritenute fuorvianti rispetto ad alcune attività di trattamento dei dati.

8 GDPR, ovvero la normativa attuativa nazionale), nonché di informative chiare rispetto all'uso e riuso delle informazioni conferite durante la navigazione nella piattaforma a fini di addestramento degli algoritmi del sistema di decisione automatizzato. Come noto, il servizio è stato ripristinato in Italia qualche settimana dopo, previa valutazione dei rischi, avviata congiuntamente tra titolare del trattamento e autorità, che, al completamento dell'istruttoria, ha portato quest'ultima a comminare una sanzione pecuniaria di quindici milioni di euro ⁽²⁷⁾.

La vicenda ha evidenziato come fosse urgente un intervento normativo volto a obbligare i prestatori di servizi digitali a valutare i rischi e le opportunità rispetto ai meccanismi decisionali automatizzati e il ruolo del GDPR come pilastro della strategia europea dei dati capace di proteggere — attraverso l'analisi dei flussi di dati personali — gli utenti rispetto ai più generali obblighi di *accountability* e trasparenza che pongono la persona e i relativi diritti fondamentali al centro di ogni iniziativa che veda l'introduzione di nuove metodologie di trattamento delle informazioni. Se Open AI avesse effettuato una valutazione di impatto più attenta, come richiesto ai sensi dell'art. 35 GDPR, avrebbe senz'altro introdotto *by design* e *by default* quelle misure minime di salvaguardia tali da consentire al soggetto interessato/utente di essere maggiormente consapevole delle implicazioni dell'accettazione dei termini e condizioni d'uso del servizio rispetto alle attività di trattamento condotte sui dati che lo riguardano e di consentirgli, di conseguenza, di esercitare i propri diritti. In ogni caso, in qualità di titolare del trattamento, l'azienda avrebbe potuto consultare preventivamente l'autorità garante ai sensi dell'art. 36 GDPR al fine di verificare con quali misure poter abilitare un trattamento sicuro per tutti i potenziali utenti del servizio proposto ⁽²⁸⁾.

⁽²⁷⁾ Con comunicazione del 28 aprile 2023, il servizio ChatGPT è stato ripristinato. In particolare, la piattaforma ha articolato una procedura più facilmente accessibile per consentire all'utente di esercitare il diritto di opposizione al trattamento dei dati; nella pagina web è stata pubblicata un'informativa sulla *privacy* dettagliata anche per i dati processati al fine di addestrare l'algoritmo, infine, sono stati sviluppati specifici meccanismi per consentire agli utenti di cancellare e/o correggere eventuali inesattezze rispetto alle informazioni trattate. Con provvedimento del 2 novembre 2024, comunicato in data 20 dicembre 2024, OpenAI è stata condannata al pagamento di una sanzione pari a 15 milioni di euro, <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10085432>.

⁽²⁸⁾ P. GUARDA - G. BINCOLETTI, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023.

Allo stesso tempo, occorre rilevare come la limitazione del servizio ChatGPT abbia riguardato, *ratione materiae*, le sole criticità sollevate rispetto alla tutela dei dati personali e della *privacy* degli utenti, non essendo possibile indirizzare altri rischi non ancora oggetto di regolamentazione nella specifica normativa di settore (si pensi all'annoso dibattito sulla responsabilità da prodotti sviluppati sulla base di tecniche di intelligenza artificiale) ⁽²⁹⁾.

Un'ulteriore questione scaturita dal caso ChatGPT (e che diventa particolarmente rilevante nella valutazione degli interventi di politica del diritto) è quella relativa alla mancata consapevolezza da parte degli utenti della sussistenza di determinati rischi e delle relative ricadute nella dimensione digitale: la mancanza di trasparenza rispetto ai profili di protezione dei dati personali non costituisce *per se* un deterrente ad aderire alla piattaforma, in quanto la gratuità del servizio è percepita in termini di innocuità, in ragione delle attuali tutele accordate dai nostri sistemi giusprivatistici.

3. **Gratuità e affidabilità: quali strumenti di tutela per gli utenti inconsapevoli?**

La datificazione della società introduce nuove variabili di mercato: le strategie di *marketing* e di *business* sono orientate a profilare gli utenti-consumatori, studiandone i comportamenti e le attitudini, al fine di proporre nuove offerte e prodotti, inducendo a perseguire certe condotte commerciali piuttosto che altre ⁽³⁰⁾.

Il limite tra strategie digitali lecite (e non) è oggetto di studio, sia in termini di pratiche commerciali scorrette e di aderenza ai principi espressi nel c.d. diritto dei consumatori, sia in termini di trasparenza e

⁽²⁹⁾ Regolamento UE, 13 giugno 2024, n. 1689, *cit.* da leggersi congiuntamente ai principi espressi dalla più recente Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio (Testo rilevante ai fini del SEE).

⁽³⁰⁾ J. RIFKIN, *The Age of Access: The New Culture of Hypercapitalism*, Penguin Putnam Inc, 2001; J. FAIRFIELD-C. ENGEL, *Privacy as a Public Good*, 2015, 65 Duke Law Journal, 385 s.

liceità dei contenuti digitali e dell'uso proprio o meno di tecniche basate sull'intelligenza artificiale nell'ambito di piattaforme *online* ⁽³¹⁾.

Ciò che rileva ai nostri fini è la sfida che il diritto privato si trova oggi ad affrontare rispetto alla declinazione del tradizionale paradigma a tutela del consumatore. Quest'ultimo, infatti, è basato sulla necessità di riequilibrare il rapporto contrattuale in ragione della asimmetria informativa che impone agli operatori di mercato obblighi di trasparenza, termini e condizioni al fine di far esercitare il recesso, strumento principe recepito nel nostro ordinamento dal D.lgs. 6 settembre 2005, n. 206, all'indomani dei numerosi interventi del legislatore europeo in materia ⁽³²⁾. Nella dimensione digitale il recesso appare non più sufficiente a ovviare ad eventuali condotte abusive e ripristinare l'equilibrio contrattuale in favore del consumatore. Far venir meno il diritto alla controprestazione senza oneri — in presenza di scenari che rendono particolarmente difficile mantenere il controllo sull'operazione economica in atto — non costituisce una misura efficace rispetto alla

(31) F. DI PORTO - A. EGBERS, *The collective welfare dimension of dark patterns regulation*, in *European Law Journal*, 2024, vol. 29, p. 114 s.; R. PARDOLESI - A. DAVOLA, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i 'dark pattern')*: *parallele convergenti?* cc.dd. *dark patterns*, in *Foro it.*, 2021, c. 338.

(32) Con particolare riferimento ai seguenti interventi: Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, direttiva UE 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, direttiva UE 2019/771, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento (UE) 2017/2394 e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE, e ai precedenti, direttiva 85/374/CEE, elativa al ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi, direttiva 85/577/CEE in materia di contratti negoziati fuori dei locali commerciali; direttiva 84/450/CEE in materia di pubblicità ingannevole, direttiva 90/314/CEE concernente i viaggi, le vacanze ed i circuiti tutto compreso, direttiva 93/13/CEE concernente le clausole abusive nei contratti stipulati con i consumatori ed in particolare l'articolo 25, e successive modificazioni, direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza, direttiva 98/7/CE, che modifica la direttiva 87/102/CEE, in materia di credito al consumo, direttiva 97/55/CE, che modifica la direttiva 84/450/CEE, in materia di pubblicità ingannevole e comparativa, direttiva 98/6/CE relativa alla protezione dei consumatori, in materia di indicazione dei prezzi offerti ai medesimi, direttiva 1999/44/CE su taluni aspetti della vendita e delle garanzie di consumo.

compromissione dei diritti degli utenti-consumatori *online* ⁽³³⁾. Si osserva, tuttavia, che anche le altre forme di tutela — sempre ispirate a preservare l'operazione economica principale, mediante il mantenimento del vincolo contrattuale ed escluse le sole condizioni imposte dal contraente forte e considerate abusive, capaci di riequilibrare l'accordo attraverso l'istituto della nullità che renda quest'ultime *tamquam non essent* — appaiono altrettanto inadeguate a soddisfare le esigenze emergenti nel mercato dei servizi e prodotti digitali. Le caratteristiche dei servizi e prodotti della società dell'informazione, infatti, soffocano la portata applicativa dei rimedi tradizionali legati al paradigma proprietario o possessorio, in quanto le dinamiche contrattuali sono mosse a privilegiare meccanismi di accesso come forma di esecuzione ⁽³⁴⁾.

Del tutto fuorviante, peraltro, è pensare di esaurire la tutela dell'utente *online* con gli strumenti forniti dalla normativa sulla *privacy*, considerando l'informazione personale il bene da tutelare al pari del patrimonio: la mera revoca del consenso (ovvero l'opposizione) al trattamento dei dati non ha la medesima efficacia del recesso nella fornitura di beni o servizi. Restando, infatti, salvi i trattamenti dei dati personali effettuati prima della revoca/opposizione, di fatto, il rimedio all'eventuale trattamento abusivo del dato personale non ripristina in alcun modo lo stato antecedente al trattamento ⁽³⁵⁾. Ciò significa che l'esercizio dei diritti da parte del soggetto interessato non potrà restituire un controllo sull'informazione precedentemente processata ed eventualmente conferita a terzi. Il controllo del soggetto interessato sul flusso di dati generato (o conferito nella dimensione digitale) si vanifica nel momento stesso in cui si aderisce ad un servizio o si utilizza un prodotto.

Occorre, dunque, indirizzare la vulnerabilità dell'utente consumatore non solo attraverso la possibilità di revocare il consenso o esercitare il diritto di opposizione al trattamento *ex post*, ma attuare tutele

⁽³³⁾ E. BACCIARDI, *Il recesso del consumatore nell'orizzonte delle scienze comportamentali*, Giappichelli, 2019; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018.

⁽³⁴⁾ C. SGANGA, *Limiti e limitazioni al diritto d'autore nel nuovo EU Data Package: alla ricerca del sistema perduto*, AIDA, 2023, p. 338 ss. In senso critico sulla crisi delle categorie giuridiche A. GENTILI, *Crisi delle categorie e crisi degli interpreti*, in *Riv. dir. civ.*, 4, 2021, p. 653.

⁽³⁵⁾ G. ZANFIR-FORTUNA, *Article 21 Right to object*, in C. KUNER *et al.* (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, 2020, Oxford Academic, <https://doi.org/10.1093/oso/9780198826491.003.0054>.

specifiche prima del conferimento dell'informazione, *by design*, ovvero identificando meccanismi capaci di illustrare *a priori* le dinamiche dei flussi di dati in modo che vi sia consapevolezza di ciò che resta e di ciò che sarà trattato, anche in caso di cessazione del rapporto contrattuale o di recesso dal servizio.

Prende così forma il concetto di affidabilità, legato a requisiti di trasparenza e governo dei flussi che dovrebbe costituire, rispetto a utenti consapevoli, il *discrimen* per la valutazione consapevole circa l'adesione o meno a determinati servizi digitali. Ed è sulla base di questo specifico profilo che è valutata la capacità di discernimento del sedicente, ai sensi dell'illustrato art. 8 GDPR, sebbene i pericoli della perdita del controllo sulle informazioni conferite (o generate *online*) siano giammai completamente noti, potendosi al più prevedere condizioni ed elaborazioni ricorrenti per le finalità dichiarate.

A fronte del rischio di perdita del controllo dell'informazione personale conferita e, dunque, del relativo riuso improprio (e abuso), invero, è l'educazione digitale a costituire la chiave di volta per valutare consapevolmente l'impatto dell'adesione a un servizio *online*, soprattutto se l'accesso allo stesso risulta gratuito e disinnesca le tutele codicistiche per gli incapaci. La sfida è individuare un meccanismo di valutazione del livello di educazione digitale che possa innescare meccanismi di presunzione di utilizzo diligente e responsabile dei servizi della società dell'informazione ⁽³⁶⁾.

La fragilità del consumatore digitale — non consapevole delle implicazioni di una determinata sessione di navigazione sul *web* — diventa una vulnerabilità universale raramente protetta a monte da un quadro regolatorio, se non per i profili strettamente legati all'applicazione della normativa sulla *privacy*, che impone obblighi specifici per i titolari di trattamento ⁽³⁷⁾. La capacità dell'utente di discernere quale servizio sia affidabile e quale invece presenti il rischio di perdita di controllo sulle informazioni trattate, laddove manchi un impatto diretto sulla sfera patrimoniale dell'utente, è — non solo sottovalutata —

⁽³⁶⁾ J. ANGRIST, P. HULL, C. WALTERS, *Methods for measuring school effectiveness*, in E. A. HANUSHEK, S. MACHIN, L. WOESSMANN (eds), *Handbook of the Economics of Education*, Elsevier, Volume 7, 2023, Ch.1,

⁽³⁷⁾ B. V. ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019.

ma considerata del tutto irrilevante rispetto alla solidità dei rapporti sinallagmatici ⁽³⁸⁾.

In questo contesto, la contezza dell'utente adolescente e quella dell'adulto appaiono del tutto assimilabili, se non addirittura da considerarsi più solida nel primo, ormai nativo digitale, piuttosto che nel secondo. Emergono, poi, nuove scale di vulnerabilità ⁽³⁹⁾, che vanno ad incidere su una pluralità di profili: dalla valorizzazione di una preferenza, alla promozione di un'attitudine, fino allo sfruttamento di una dipendenza ⁽⁴⁰⁾. Ad esse, tuttavia, si accompagnano nuove opportunità di accesso paritario a servizi e prodotti per soggetti altrimenti vulnerabili nell'ambiente fisico: si pensi alle implicazioni positive della digitalizzazione sull'abbattimento delle barriere socio-economiche, sulla vanificazione dei confini geografici, sulla circoscrizione delle differenze linguistiche e sulla promozione di misure a sostegno delle disabilità, che potenziano l'accesso alla conoscenza e all'inclusività.

Costruire un sistema di tutele integrate per la pluralità di utenti necessita numerosi sforzi di armonizzazione rispetto ad una pluralità di elementi tra cui: il ruolo della datificazione nella normativa di settore ⁽⁴¹⁾, le variabili di conformità introdotte dalla strategia europea sui dati sulla base del principio di *accountability*, i necessari accomodamenti per prevenire effetti pregiudizievoli su individui e gruppi di individui portatori di determinati interessi specifici ed emergenti dalle valutazioni di impatto ⁽⁴²⁾, etc.

⁽³⁸⁾ C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, R. GIARDA, J. LIOTTA, G. RINDI, *Vita quotidiana del minore online. Tra esigenze di tutela e limiti tecnologici*, cit.

⁽³⁹⁾ G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford University Press, April 2023.

⁽⁴⁰⁾ L. GATT, I. CAGGIANO, *Consumers and Digital Environments as a Structural Vulnerability Relationship* (2022) 2 EJPLT, 8-16. DOI: <https://doi.org/10.57230/EJPLT222LGIAC>.

⁽⁴¹⁾ Si pensi a tal proposito alle iniziative europee in materia di governo dei dati, nei servizi digitali e nei mercati digitali, su cui *infra* §§ 4 e 5.

⁽⁴²⁾ Vedremo nei prossimi paragrafi come le iniziative in materia di dati attribuiscono agli operatori economici il compito di valutare in concreto le vulnerabilità e le misure per mitigare i rischi di compromissione dei diritti fondamentali della persona. Sia concesso rinviare a D. AMRAM, *Standards to Face Children and Patients Digital Vulnerabilities*, in C. CREA-A. DE FRANCESCHI (eds), *The New Shapes of Digital Vulnerability in European Private Law*, cit., pp. 439 e EAD, *Comparing EU Initiatives on Data: Addressing Risks and Enhancing Harmonisation Opportunities*, in *Opinio Juris in Comparatione*, 2023, 1 ss.

Come è emerso nel caso di ChatGPT, infatti, le criticità sollevate dall'analisi dell'informativa e del documento illustrante i termini e le condizioni d'uso del servizio non hanno per nulla evitato l'utilizzo del sistema da parte di qualsiasi tipologia di utente. Le potenzialità e le opportunità fornite dal *software* — non a caso a titolo gratuito — hanno determinato (e determinano) un progressivo affidamento *tout court* assumendo che — non comportando pericolo all'assetto patrimoniale dell'utente — l'adesione senza riserve (o con riserve superabili dalle peculiarità del servizio) è di fatto giustificata e promossa ⁽⁴³⁾.

Per tale ragione, accanto all'introduzione di obblighi di misurazione, mitigazione e monitoraggio dei rischi percepiti come conseguenze dirette o indirette di una iniziativa basata sul trattamento di dati personali (e non), occorre introdurre strumenti di sensibilizzazione e formazione volti a irrobustire le competenze e la consapevolezza delle persone, affinché possano agire in maniera responsabile ⁽⁴⁴⁾.

A questo proposito, l'approccio del legislatore europeo basato sulla valutazione del rischio da prevenire *by design* e *by default*, introduce meccanismi di responsabilizzazione, oltre che di responsabilità, degli operatori.

In particolare, il modello si articola in una pluralità di iniziative, tra cui lo schema adottato dal GDPR, che impone l'obbligo di valutare l'impatto di una determinata attività di trattamento rispetto alla persona umana e ai relativi diritti fondamentali, seguendo una specifica procedura laddove lo stesso, in ragione del mezzo "*in particolare l'uso di nuove tecnologie*" e "*considerati la natura, l'oggetto, il contesto e le finalità del trattamento*" possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche ⁽⁴⁵⁾.

⁽⁴³⁾ S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019, New York, Public Affairs. Sulle statistiche si vedano alcuni dati relative a ChatGPT: K. HU, *ChatGPT sets record for fastest-growing user base* - analyst note, 2 febbraio 2023, Reuters, in <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>; K. O' FLAHERTY, *ChatGPT-4o Is Wildly Capable, But It Could Be A Privacy Nightmare*, Forbes, 17.5.2024, <https://www.forbes.com/sites/kateoflahertyuk/2024/05/17/chatgpt-4o-is-wildly-capable-but-it-could-be-a-privacy-nightmare/>.

⁽⁴⁴⁾ Su cui *infra* Cap. 3.

⁽⁴⁵⁾ A. CALVI, *Data Protection Impact Assessment under the EU General Data Protection Regulation: A feminist reflection*, in *Computer Law & Security Review*, Volume 53, 2024, 105950, <https://doi.org/10.1016/j.clsr.2024.105950>; M. FRIEDEWALD, I. SCHIERING, N. MARTIN, D. HALLINAN, (2022). *Data Protection Impact Assessments in*

L'intento del legislatore appare quello di innescare, a cascata, un processo virtuoso che metta, sin da subito, l'utente nelle condizioni di poter superare i limiti dovuti all'asimmetria informativa e all'educazione digitale, potendo in ogni caso assumere scelte consapevoli e non lesive dei propri interessi, anche laddove la controprestazione non si configuri in un trasferimento di denaro e, dunque, in un depauperamento economico del singolo. Non è un caso, infatti, che il principio di trasparenza costituisca uno dei cardini della strategia dell'UE sui dati come premessa a rendere note le caratteristiche delle attività degli operatori della società dell'informazione e, al contempo, edotti su esse gli utenti.

4. Il Regolamento europeo sui servizi digitali: gli obblighi di trasparenza.

La creazione di uno spazio digitale affidabile e sicuro è l'obiettivo cardine del Reg. UE n. 2022/2065 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali, di seguito anche "DSA"). In particolare, l'iniziativa si propone di *"contribuire al corretto funzionamento del mercato interno dei servizi intermediari stabilendo norme armonizzate per un ambiente online sicuro, prevedibile e affidabile che faciliti l'innovazione e in cui i diritti fondamentali sanciti dalla Carta, compreso il principio della protezione dei consumatori, siano tutelati in modo effettivo"* ⁽⁴⁶⁾.

Il regolamento individua obblighi e responsabilità per tre tipologie di servizi: la trasmissione, la memorizzazione temporanea durante la trasmissione, la mera memorizzazione di informazioni fornite da un destinatario di un servizio, classificando i prestatori e i relativi obblighi a seconda della portata — ovvero del relativo volume, stabilito sulla base del numero medio di destinatari attivi — in piattaforme *online* di dimensioni molto grandi o di motori di ricerca *online* di dimensioni

Practice, in S. KATSIKAS ET AL. Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science, vol 13106. Springer, Cham. https://doi.org/10.1007/978-3-030-95484-0_25; K. DEMETZOU, *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *Computer Law & Security Review*, Volume 35, Issue 6, 2019, 105342, <https://doi.org/10.1016/j.clsr.2019.105342>.

⁽⁴⁶⁾ O. POLLICINO, *Verso il Digital Services Act: problemi e prospettive. Presentazione del simposio*, MediaLaws, 2020.

molto grandi, destinatari di tutti gli obblighi. Alle altre piattaforme, ai servizi di *hosting* e di intermediazione sono richiesti, a scalare, un numero inferiore di adempimenti in ragione del minor impatto delle attività svolte ⁽⁴⁷⁾.

A norma dell'art. 14 DSA, i servizi di intermediazione devono illustrare nell'ambito della sezione dedicata ai termini e condizioni d'uso, fra le altre, *“le politiche, le procedure, le misure e gli strumenti utilizzati ai fini della moderazione dei contenuti”*. Specificando che, in caso di processo decisionale automatizzato mediante algoritmi e validazione umana, occorre identificare procedure per amministrare i reclami da parte degli utenti. In questa norma si concentra la tutela dell'utente che dovrebbe, in ragione di documenti redatti *“in un linguaggio chiaro, semplice, comprensibile, facilmente fruibile e privo di ambiguità”*, poter colmare l'asimmetria informativa, capire le destinazioni e gli usi dei flussi informativi generati *online* e valutare le implicazioni in caso di adesione al servizio. In aggiunta, per le piattaforme e per i prestatori di servizi di memorizzazione delle informazioni occorre implementare meccanismi di segnalazione e gestione di reclami in ordine alla presenza di contenuti illeciti da gestire in maniera autonoma. Peraltro, al fine di un monitoraggio trasparente, la Commissione Europea ha attivato un cruscotto in cui riporta in tempo reale tutte le motivazioni di eventuali restrizioni e azioni che ai sensi dell'art. 17 DSA rispondono alle segnalazioni degli utenti ⁽⁴⁸⁾. Da questo emerge che restrizioni volte a proteggere i minori di età su segnalazione sono nell'ordine delle decine di migliaia al giorno, sebbene tale criticità non costituisca quella statisticamente più comune.

⁽⁴⁷⁾ In particolare, obblighi comuni a tutti sono quelli relativi alla trasparenza rispetto alla rappresentanza legale e sussistenza di punti di contatto, nonché rispetto alla pubblicazione di termini e condizioni d'uso, mentre al livello superiore è altresì richiesto di pubblicare le motivazioni rispetto alle decisioni restrittive a seguito di segnalazioni. Per le piattaforme, a prescindere dal volume, vi sono gli obblighi di *due diligence*, non applicabili in ogni caso alle micro e piccole imprese, rispetto all'introduzione di un meccanismo di gestione dei reclami, alla reportistica di reati penali, all'identificazione misure di protezione contro gli abusi, alle condizioni per proporre pubblicità *online* etc. Per le sole piattaforme di grandi dimensioni, invece, sono introdotti, sempre in maniera cumulativa ai precedenti, meccanismi di monitoraggio (anche esterno attraverso *audit*) e di reportistica periodica.

⁽⁴⁸⁾ DSA Transparency Database, disponibile su <https://transparency.dsa.ec.europa.eu/dashboard>.

4.1. (Segue). *Gli obblighi di protezione per i minori di età.*

Il DSA presta attenzione agli utenti minorenni introducendo norme specifiche per tutelare e promuovere i diritti fondamentali dell'infanzia nella dimensione digitale.

In particolare, l'articolo 28 DSA stabilisce un obbligo per i fornitori di piattaforme *online* che siano accessibili (e non dunque destinate esclusivamente o prioritariamente) a minori di età di adottare misure “*adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio*”. Salvo il supporto mediante emanazione di orientamenti e buone prassi da parte della Commissione, spetta al fornitore effettuare per il proprio spazio nell'ambiente digitale una valutazione di impatto che vada a declinare i rischi relativi ai profili enucleati.

In particolare, si osserva quanto segue. Il legislatore europeo si preoccupa prioritariamente di proteggere la riservatezza rispetto all'esposizione pubblica di contenuti relativi alla vita privata. A questo proposito, la valutazione di impatto introdotta nel DSA sopperirebbe a quei limiti di percezione e contezza dovuti all'immaturità dell'utente in termini di capacità di discernere le conseguenze delle condotte al fine di assicurare l'affidabilità e sicurezza della piattaforma o dello specifico spazio digitale.

Il secondo profilo di tutela concerne, poi, la sicurezza, da intendersi come “robustezza” — nei termini indicati per la valutazione dei meccanismi basati sull'intelligenza artificiale ⁽⁴⁹⁾. In particolare, nel DSA l'attenzione è rivolta alla protezione della sicurezza personale, al fine di introdurre misure di prevenzione all'eventuale esposizione a rischi concernenti la vita, la salute, l'integrità fisica, cagionati dal *cyberbullismo* con condotte che portano a compromettere il benessere dell'utente attraverso sfide e giochi che mettono in pericolo l'incolumità dell'utente stesso ⁽⁵⁰⁾. Infine, nel DSA il riferimento alla sicurezza è da intendersi altresì come strumento per la protezione del singolo utente in quanto appartenente ad una categoria di soggetti vulnerabili, proprio in ragione della serietà delle conseguenze pregiudizievoli che

⁽⁴⁹⁾ AI High Level Expert Group, *Assessment List on Trustworthy AI*, 2020, <https://digital-strategy.ec.europa.eu/it/node/806>, su cui, *infra* §7.1.

⁽⁵⁰⁾ Ci si riferisce alle “challenges” come Blue Whale o Black Out per le quali l'Autorità Garante della Concorrenza e del Mercato ha avviato istruttorie, comminando — ad esempio — sanzioni per pratiche commerciali scorrette, come per la piattaforma Tik Tok: <https://www.agcm.it/media/comunicati-stampa/2024/3/PS12543->.

possono verificarsi sull'individuo maggiormente esposto a pericoli per una propria condizione personale. In questa accezione si ravvisa una forma di attuazione del principio internazionalmente riconosciuto del perseguimento dell'interesse superiore del fanciullo, da declinarsi in ottica preventiva come divieto di arrecare qualsivoglia forma di nocuo-mento agli utenti minori di età. Tra gli esempi rappresentativi di questa accezione si enucleano, da un lato, la lotta alla disinformazione, che costituisce una misura di tutela anche per l'autodeterminazione e lo sviluppo del pensiero dei soggetti minori di età, al fine di evitare di plasmare la loro crescita e capacità di discernimento su premesse e argomentazioni false ⁽⁵¹⁾. Dall'altro lato, la norma include un espresso divieto di profilazione ⁽⁵²⁾, laddove vi sia ragionevole consapevolezza che l'utente sia minorenne, con il limite esplicito per il titolare del trattamento prestatore del servizio del divieto di acquisizione di dati personali al mero fine di accertare l'età, laddove — ad esempio — l'accesso alla piattaforma non richieda l'apertura di un profilo individuale ⁽⁵³⁾.

Da osservare, alla luce delle riflessioni condotte nei paragrafi precedenti, che la definizione di minore di età nel DSA coincide presuntivamente con quella indicata dalla Convenzione sui diritti dell'infanzia e dell'adolescenza (di seguito anche "CRC") ⁽⁵⁴⁾: ovvero ogni volta che il DSA si riferisce al minore di età intende coloro che non abbiano compiuto anni 18. Tale interpretazione trova giustificazione nel richiamo all'art. 24 della Carta dei Diritti Fondamentali dell'UE,

⁽⁵¹⁾ Il Considerando 104 DSA, in particolare, si occupa di evidenziare come l'adesione a codici di condotta che introducano meccanismi di individuazione di contenuti abusivi, come l'utilizzo di bot o profili falsi volti alla creazione e condivisione di informazioni intenzionalmente inesatte o fuorvianti, talvolta anche a scopo di lucro, debba essere effettiva, non essendo sufficiente la mera dichiarazione per presumere la conformità al Regolamento.

⁽⁵²⁾ R. BINNS, M. VEALE, *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, in *International Data Privacy Law*, Volume 11, Issue 4, November 2021, p. 319 <https://doi.org/10.1093/idpl/ipab020> e G. MALGIERI, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in *Computer Law & Security Review*, Volume 35, Issue 5, 2019, 105327, <https://doi.org/10.1016/j.clsr.2019.05.002>.

⁽⁵³⁾ La formula del divieto di profilazione relativizzato rispetto all'acquisizione di ulteriori informazioni personali è presente in maniera ridondante anche nei *consideranda*.

⁽⁵⁴⁾ Convenzione ONU sui diritti dell'infanzia e dell'adolescenza, *cit.*.

che a sua volta cita le Convenzioni internazionali e la Carta delle Nazioni Unite in seno al proprio articolo 3, comma 5 ⁽⁵⁵⁾.

Al di là del dato letterale, ciò che rileva, più in particolare, in questa sede è che le tutele specifiche previste per i minorenni siano indirizzate a prescindere dal fatto che l'infrasedicenne possa, a norma dell'art. 8 GDPR o della normativa nazionale, esprimere un valido consenso al trattamento dei dati conferiti nell'ambito di servizi della società dell'informazione ⁽⁵⁶⁾. Con riferimento ai contenuti *online* per i servizi che si rivolgono principalmente ai minori di età occorre, pertanto, procedere ad una valutazione "adattata" ⁽⁵⁷⁾ ai rischi specifici che siano stati identificati per quella categoria di utenti.

A chiarire quali siano i profili di criticità da analizzare nell'ambito della valutazione con le lenti dei minori spetta ai *consideranda* del DSA che, tuttavia, forniscono indicazioni di massima, senza descrivere le criticità da indirizzare.

Il considerando 71, infatti, esemplifica le misure tecniche ed organizzative che le piattaforme online potrebbero utilizzare per proteggere i diritti dei minori: *in primis*, l'accesso ad utenti minorenni dovrebbe essere espressamente autorizzato nelle condizioni generali del servizio. Ciò si allinea con il considerando 46 DSA che, nel richiamare il principio di trasparenza, intima agli intermediari digitali di rendere la documentazione relativa alle condizioni e termini d'uso alla portata (*rectius* a misura) dei bambini, laddove questi ultimi siano gli utenti prevalenti, vuoi per ragioni inerenti la progettazione, vuoi per la commercializzazione dei servizi stessi.

Secondariamente, lo stesso considerando 71 richiama l'adesione a codici di condotta per definire gli *standard* relativi al "*massimo livello di privacy, sicurezza e protezione dei minori per impostazione predefinita*" da implementare nelle interfacce e nei sistemi, ovvero per individuare le buone prassi disponibili dalle strategie della Commissione Europea,

⁽⁵⁵⁾ L'IA act, invece, specifica al considerando 9 che per soggetti minori di età si intendano coloro che non abbiano compiuto i diciotto anni di età.

⁽⁵⁶⁾ M. CANTERO GAMITO-H. W. MICKLITZ, *Too much or too little? Assessing the Consumer Protection Cooperation (CPC) Network in the protection of consumers and children on TikTok* (BEUC, 17-02-23) https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf.

⁽⁵⁷⁾ L'espressione richiama il noto saggio F. GIARDINA, *Per un'indagine sulla responsabilità civile nella famiglia. L'art. 129-bis del codice civile*, Pisa, ETS, 1999.

indicando come esempio virtuoso il programma “BIK +” ⁽⁵⁸⁾. Il considerando 81 stabilisce che per le piattaforme e motori di ricerca *online* di dimensioni molto grandi la valutazione di impatto debba basarsi sui seguenti parametri: *i)* facilità per i minori di comprendere la progettazione e il funzionamento del servizio, che presuppone la possibilità di parametrare gli obblighi di trasparenza a livelli differenziati di educazione e alfabetizzazione digitale oltre che di capacità di discernimento; *ii)* esposizione a contenuti pregiudizievoli per la loro salute o al loro sviluppo fisico, mentale e morale, come antecedente logico all’uso improprio e non supervisionato dei servizi digitali. In particolare, i meccanismi volti a sfruttare “*intenzionalmente o involontariamente le debolezze e l’inesperienza dei minori o che possono causare comportamenti di dipendenza*” debbono essere vietati ⁽⁵⁹⁾. Tale divieto trova concreta attuazione, tuttavia, solo *ex post* in ottemperanza di un ordine di contrastare contenuti illegali o previa segnalazione ovvero reclamo da parte di utenti, ovvero in ottica preventiva il prestatore di servizi potrebbe escludere l’accesso a determinati contenuti ai minori di età. Coerentemente con questo schema, il considerando 89 sollecita l’implementazione di misure per consentire un facile accesso ai meccanismi di reportistica e segnalazione, ovvero raccomanda la pubblicazione di condizioni e sbarramenti a contenuti pregiudizievoli. A tal fine, il DSA suggerisce di analizzare anche le pratiche di raccolta e utilizzo dei dati e il modo in cui i servizi stessi sono “*utilizzati per diffondere o*

⁽⁵⁸⁾ La strategia europea per una migliore Internet per i bambini è stata lanciata nel maggio 2022 e individua tre pilastri: il primo relativo all’assicurare l’interesse superiore dei bambini, in quanto giovani consumatori, attraverso esperienze digitali sicure; il secondo riguardante la responsabilizzazione digitale in modo da offrire a tutti i bambini, anche quelli in situazioni di vulnerabilità, pari opportunità in termini di capacità e competenze necessarie per essere utenti consapevoli; il terzo relativo alla promozione della partecipazione attiva dei bambini sulle politiche in materia di innovazione e digitalizzazione, <https://digital-strategy.ec.europa.eu/it/policies/strategy-better-internet-kids>. Anche il Considerando 102 DSA incoraggia forme di auto-regolamentazione per identificare buone prassi e *standard* a tutela dei minori di età.

⁽⁵⁹⁾ Si pensi al caso presentato alla Corte distrettuale della Florida, *Garcia v. Character Technologies, Inc.* (6:24-cv-01903), relativa al caso del quattordicenne suicida, convinto di intrattenere una relazione affettiva con un *chatbot*. Sui diritti dei minori e piattaforme digitali K. KAESLING (2023). *A Rights-Based Approach to Children’s Digital Participation in the Multi-Level System of the European Union*, in N. DETHLOFF, KAESLING, K., L. SPECHT-RIEMENSCHNEIDER (eds), *Families and New Media. Juridicum - Schriften zum Medien-, Informations-und Datenrecht*. Springer, Wiesbaden. https://doi.org/10.1007/978-3-658-39664-0_4.

amplificare contenuti fuorvianti o ingannevoli, compresa la disinformazione”.

In questo contesto di inviti e raccomandazioni, peraltro, si inseriscono le valutazioni di impatto laddove siano coinvolti processi decisionali automatizzati: nella specie occorre riferirsi a quella prevista in materia di trattamento di dati personali, a quella relativa ai sistemi di profilazione e a quella sull'impatto delle risultanze del sistema di IA in termini di possibile condivisione di contenuti portatori di effetti distortivi o manipolatori della realtà o, in ogni caso, che mettano in pericolo l'incolumità e sicurezza dell'utente ⁽⁶⁰⁾. Spetta alla piattaforma, infatti, prevenire, evitare e limitare con diligenza ⁽⁶¹⁾ comportamenti (anche solo parzialmente) automatizzati che portino ad un uso non autentico o ingannevole del servizio ⁽⁶²⁾, mediante — ad esempio — adattamenti nei meccanismi di moderazione e segnalazione. In questo senso, il considerando 62 DSA contiene una raccomandazione ad utilizzare i segnalatori attendibili per la moderazione di contenuti che non siano in contrasto con le condizioni e termini d'uso, ovvero lesivi dei diritti dei soggetti vulnerabili, tra cui i minori.

Tutti questi accorgimenti tecnici e organizzativi esplicitano la formula contenuta nell'art. 55 DSA lett. j) che impone l'adozione di “*misure mirate*” alla protezione degli utenti minori di età. Queste ultime possono riguardare sia strumenti di verifica dell'età, senza procedere — come accennato — a ulteriori raccolte di dati personali, sia meccanismi che introducano forme di controllo parentale, al fine di limitare la diretta esposizione a determinati contenuti, o a monitorare la navigazione dell'utente in termini anche temporali, sia sistemi volti a controllare l'identificazione dell'utente tanto per supportare la segnalazione di eventuali abusi, quanto per chiedere possibile aiuto ai moderatori dei sistemi.

⁽⁶⁰⁾ La valutazione di impatto ai sensi dell'art. 35 GDPR riguarda l'individuazione e misurazione dei rischi rispetto alla confidenzialità, integrità e disponibilità dei flussi, mentre la valutazione dei processi decisionali automatizzati misura l'affidabilità di un sistema basato sull'intelligenza artificiale nel processare informazioni e inferire nuova conoscenza, che a sua volta è una valutazione diversa dalle implicazioni dell'esposizione a determinati contenuti offerti dai servizi digitali. La matrice complessa di obblighi di valutazione di impatto imposti dalle diverse normative di settore richiede in primo luogo di procedere per gradi individuando l'oggetto di ciascuna valutazione e le relative interrelazioni.

⁽⁶¹⁾ Considerando 86.

⁽⁶²⁾ Considerando 84.

Nel considerando 52, invero, il legislatore europeo enuclea una pluralità di possibili pericoli per introdurre variegate misure di protezione senza, tuttavia, ricorrere ad una sistematizzazione delle categorie di diritti elencati. La norma si riferisce, infatti, alla protezione della dignità umana, ai diritti dei minori di età, alla tutela della proprietà — specificando per quest’ultima di includere anche (o sarebbe meglio chiedersi se voler richiamare *soprattutto*) quella intellettuale — e alla tutela del pluralismo, menzionando, in particolare, il diritto alla non discriminazione. L’esemplificazione di alcune categorie è foriera di possibili dubbi interpretativi, laddove il legislatore europeo avrebbe potuto semplicemente richiamare in maniera omnicomprensiva i diritti fondamentali della Carta di Nizza, esplicitando — però — specifiche linee di intervento verso la tutela dei soggetti deboli e delle minoranze. L’approccio adottato, invero, dal carattere meno dogmatico e più pratico, appare strumentale ad ammonire i prestatori di servizi digitali, affinché valutino i rischi associati a tali profili, onde evitare che un obbligo di protezione troppo generale e generalizzato porti ad una superficiale attività di analisi delle esposizioni a condotte notoriamente pregiudizievoli per l’utente o per determinate categorie di utenti. Di fatto, il processo di responsabilizzazione degli operatori appare passare anche dall’esemplificazione — non tassativa, né tanto meno esaustiva — di scenari che non possono non essere, di conseguenza, percepiti quali fattori di rischio, in quanto è il legislatore stesso ad indirizzare verso quei profili di criticità.

5. Le ricadute su specifiche normative di settore: il Regolamento sui mercati digitali.

Le norme sul DSA trovano complementare corrispondenza nel di poco precedente Regolamento sui mercati digitali 2022/1925 del 14 settembre 2022 (di seguito anche “DMA”, dalla formulazione inglese Digital Markets Act) ⁽⁶³⁾.

Quest’ultimo si pone l’obiettivo di garantire “*la contendibilità e l’equità*” sia per i mercati, che per gli utenti commerciali e gli utenti finali nella dimensione digitale, contribuendo al corretto funziona-

⁽⁶³⁾ Reg. UE, 14 settembre 2022, n. 1925, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

mento del mercato interno ⁽⁶⁴⁾ ed evitando la frammentazione emergente — anche al livello nazionale — da normative di settore. L'intervento normativo, in particolare, impone condizioni per rendere i servizi offerti dalle piattaforme *gatekeeper* interoperabili per i terzi, per consentire agli utenti commerciali di accedere ai dati generati e di promuovere e concludere contratti con clienti al di fuori della piattaforma stessa e agli inserzionisti ed editori di effettuare verifiche indipendenti sulla pubblicità ⁽⁶⁵⁾.

Il DMA, dunque, non si occupa direttamente della protezione dei minori di età, ma al considerando 38 raccomanda la conformità al sistema di garanzie per questa categoria di soggetti vulnerabili previste dalle norme dell'Unione Europea. In particolare, esclude che le piattaforme di grandi dimensioni che operano quali *gatekeeper*, ovvero che forniscono punti di accesso “*a un gran numero di utenti commerciali per raggiungere gli utenti finali in tutta l'Unione e su mercati diversi*” ⁽⁶⁶⁾, possano essere esonerati da specifici obblighi verso i minori di età nella costruzione di un mercato unico per i servizi digitali, soprattutto con riferimento, ancora una volta, agli scenari che devono essere sviscerati in sede di valutazione di impatto: l'uso dei relativi dati personali rispetto alle ipotesi di comunicazione commerciale e la creazione di profili utente.

Questi due aspetti lasciano intendere tutto ciò che è confluito nel GDPR in termini di consenso al trattamento per i servizi della società dell'informazione ai sensi dell'art. 8 GDPR in combinato disposto con le condizioni previste per la profilazione *ex art.* 22 GDPR ⁽⁶⁷⁾. Inoltre, gli obblighi di protezione illustrati nel successivo intervento normativo sui servizi digitali (DSA) sono da considerarsi applicabili in termini di responsabilizzazione, alla luce dei principi di *accountability*, trasparenza ed equità sin da subito, e — in termini di responsabilità — una

⁽⁶⁴⁾ Così il Considerando 8.

⁽⁶⁵⁾ A.C. WITT, *The Digital Markets Act: Regulating the Wild West*, (2023), 60, Common Market Law Review, Issue 3, pp. 625-666, <https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/60.3/COLA2023047>.

⁽⁶⁶⁾ Così il Considerando 6.

⁽⁶⁷⁾ G. MALGIERI - G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law* 7, no. 4, 2017: 243-65, <https://doi.org/10.1093/idpl/ipx019> e G. MALGIERI, *The vulnerable data subject in the GDPR, Vulnerability and Data Protection Law*, cit. <https://doi.org/10.1093/oso/9780192870339.003.0004>.

volta allineate le tempistiche di approvazione, entrata in vigore e attuazione delle due diverse normative.

5.1. (Segue). *La regolamentazione dei contenuti audiovisivi.*

Nell'ambito della strategia per un mercato digitale unico in Europa, lanciata dalla Commissione Europea nel 2015 ⁽⁶⁸⁾, uno dei primi interventi ha interessato la parziale modifica della direttiva sui servizi di media audiovisivi Dir. UE 2010/13/UE ⁽⁶⁹⁾, mediante Direttiva UE 2018/1818 ⁽⁷⁰⁾. Quest'ultima si propone di regolamentare le piattaforme di condivisione video e contenuti audiovisivi disponibili su determinati servizi di *social media*, proteggendo i minori di età e, in particolare, rafforzando la lotta contro i discorsi di incitamento all'odio ⁽⁷¹⁾.

La Direttiva promuove una armonizzazione minima tra servizi di trasmissione televisiva e servizi di media audiovisivi a richiesta. In particolare, per i fornitori di servizi di media sono previsti obblighi di trasparenza al fine di *“permettere ai telespettatori, compresi i genitori e i minori, di prendere decisioni informate sui contenuti da guardare”*, imponendo una valutazione rispetto al rischio, seppur non strutturata come nelle iniziative precedentemente illustrate, di recare danno allo sviluppo fisico, mentale o morale dei minori, il cui risultato assume le forme di *“un sistema di descrittori di contenuti, un'avvertenza acustica, un simbolo visivo o qualsiasi altro mezzo che descriva la natura del contenuto”* ⁽⁷²⁾. Si promuovono altresì misure tecniche, come la criptazione e controlli parentali efficaci, onde evitare l'accesso a contenuti *“maggiormente”* nocivi e misure organizzative, come codici di condotta

⁽⁶⁸⁾ <https://www.consilium.europa.eu/it/meetings/eys/2015/05/18-19/>.

⁽⁶⁹⁾ Direttiva 2010/13/UE del Parlamento europeo e del Consiglio, del 10 marzo 2010, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), <https://eur-lex.europa.eu/legal-content/IT/AUTO/?uri=celex:32010L0013>.

⁽⁷⁰⁾ Direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.

⁽⁷¹⁾ Si vedano i contributi pubblicati nel volume collettaneo N. DETHLOFF, K. KAESLING, L. SPECHT-RIEMENSCHNEIDER (a cura di) *Families and New Media*. cit.

⁽⁷²⁾ Considerando 19.

e forme di autoregolamentazione ai sensi dell'art. 4 *bis* della Direttiva. Infine, la protezione offerta in materia di media anticipa la regola cardine di raccordo tra GDPR e DSA che abbiamo poc'anzi illustrato, secondo cui, presupponendo i meccanismi di protezione dei soggetti minori di età il trattamento dei relativi dati personali, occorre escludere il riuso delle informazioni concernenti i telespettatori minorenni a fini commerciali ⁽⁷³⁾, come in caso di “*marketing diretto, profilazione e pubblicità mirata sulla base dei comportamenti*”, come meglio esplicitato all'art. 2 della Direttiva. Ulteriori raccomandazioni indirizzate agli Stati Membri per una più efficace normativa di recepimento dei principi espressi indicano, nello specifico, un divieto di esposizione dei minori di età a comunicazioni commerciali relative alle bevande alcoliche ⁽⁷⁴⁾ o al gioco d'azzardo ⁽⁷⁵⁾, nonché l'adozione di misure “proporzionate” rispetto alla lotta all'incitamento a discorsi d'odio su piattaforme che offrono servizi di condivisione di video. Appare evidente come il legislatore europeo abbia voluto introdurre degli scenari che impongano misure per prevenire ed eventualmente sanzionare forme di *cyberbullismo* ⁽⁷⁶⁾, evitando contenuti che istighino gli spettatori alla violenza, odio e terrorismo in generale ⁽⁷⁷⁾.

Il perno della tutela dei minori è previsto nell'art. 9 lett. g), che si articola in una serie di divieti, in parte già anticipati nei *consideranda*. In particolare, gli Stati Membri sono chiamati a proibire comunicazioni commerciali audiovisive considerate pregiudizievoli, ovvero non solo quelle che arrechino danno fisico, mentale o morale ai minori di età, ma anche quelle che ne sfruttino l'immatunità e la limitata capacità di discernimento (*i.e.* inesperienza e incredulità). Ciò vale tanto per quelle pratiche commerciali volte ad indurre in maniera diretta “*ad acquistare o prendere in locazione un prodotto o un servizio*”, quanto per quelle indirette, volte a “*persuadere i loro genitori o altri ad acquistare i beni o i servizi pubblicizzati*”, ovvero a “*sfruttare la particolare fiducia che i minori ripongono nei genitori, negli insegnanti o in altre persone*”,

⁽⁷³⁾ Considerando 21.

⁽⁷⁴⁾ Considerando 29.

⁽⁷⁵⁾ Considerando 30.

⁽⁷⁶⁾ Considerando 45.

⁽⁷⁷⁾ Considerando 51, che offre come soluzione l'operare di un bilanciamento in favore dei diritti fondamentali della persona, come il rispetto della vita privata e familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di impresa, il divieto di discriminazione e, quasi a ribadirne le peculiarità rispetto agli adulti, i diritti dei minori.

oppure — ancora — a incutere timore, mostrando “*senza motivo minori che si trovano in situazioni pericolose*”. In altri termini, la norma mira a mitigare gli effetti manipolativi delle pratiche commerciali, proponendo una serie di scenari che progressivamente si pongono in una posizione distorsiva rispetto alla libera formazione del pensiero e dell’opinione dello spettatore-consumatore vulnerabile, con ricadute più o meno gravi nella sfera economica, privata, affettiva ed emotiva dello stesso. Ciò che caratterizza questo sistema di tutele è la combinazione della protezione tradizionale rispetto agli atti dispositivi (come l’acquisto e la locazione di servizi e prodotti), per i quali certe pratiche potrebbero essere sanzionate in termini di annullabilità dei contratti. Infatti, dagli scenari illustrati nella disposizione, il timore incusso potrebbe assumere rilevanza, anche in assenza degli elementi di cui all’art. 1435 c.c. e quale eccezione all’art. 1437 c.c. ⁽⁷⁸⁾. Al contempo, tuttavia, la norma si pone nella prospettiva della datificazione della società, individuando un abuso nell’offerta di comunicazioni pubblicitarie che sfruttino le attitudini e i comportamenti degli spettatori sia rispetto all’uso dei servizi audiovisivi, sia rispetto alla creazione di contenuti non del tutto veritieri o manipolati attraverso tecniche di *marketing* persuasivo e volte a creare dipendenza ovvero destabilizzare le certezze del consumatore (cfr. le condotte che coinvolgono gli adulti di riferimento).

Due sono, pertanto, i piani di indagine: da un lato, la tutela dello spettatore consumatore, inteso come categoria di soggetto vulnerabile rispetto al bilanciamento da effettuare tra le condotte dei fornitori di servizi e la limitata capacità di discernimento, andando ad analizzare l’impatto sulla dignità e sulla libertà di autodeterminazione dello spettatore minorenni “medio”, onde verificare la liceità o abusività delle strategie commerciali proposte, anche a fini di accertare la validità delle operazioni commerciali intraprese; dall’altro lato, una rinnovata tutela del singolo individuo minorenni in termini di perseguimento del relativo “non nocimento”, parafrasabile come benessere, al livello fisico, mentale e morale.

La formula, che sembrerebbe richiamare le epifanie del danno alla

⁽⁷⁸⁾ A. FIGONE, *La violenza. Artt. 1434-1439 Codice Civile Commentato*, Giuffrè, 2005.

persona nella concezione tripartita del danno non patrimoniale ⁽⁷⁹⁾ e dunque definire le conseguenze della compromissione di un diritto fondamentale della persona, nella specie del bambino spettatore, in realtà apre a nuove interpretazioni che recentemente hanno portato alcuni studiosi a configurare specifiche situazioni meritevoli di tutela a sé, come i neurodiritti, consistenti nella protezione della dimensione mentale della persona rispetto alle nuove forme di sfruttamento disegnate dalle tecnologie ⁽⁸⁰⁾. Si tratterebbe, infatti, di costruire un paradigma di tutele volte a proteggere i processi cognitivi della persona da scenari di manipolazione, sorveglianza, controllo resi possibili dal progresso tecnologico.

6. (Segue). Il dibattito sulla regolamentazione dei neurodiritti.

Il dibattito sulla configurabilità di una tutela autonoma per i cc.dd. neurodiritti ha particolarmente vivacizzato il dialogo fra formanti giuridici. Ad oggi, in dottrina si ravvisano tre posizioni ⁽⁸¹⁾: una prima che individua la necessità di introdurre nuovi diritti ⁽⁸²⁾, una seconda, più moderata, che considera sufficiente l'adattamento delle interpretazioni dei diritti fondamentali della persona per indirizzare i rischi delle neurotecnologie ⁽⁸³⁾, una terza c.d. "negazionista" rispetto alle due

⁽⁷⁹⁾ G. PONZANELLI-R. FOFFA, *Il danno esistenziale (1991-2008)*, in S. DELLE MONACHE (a cura di), *Responsabilità civile. Danno non patrimoniale*, Torino, Utet Giuridica, 2010, pp. 288.

⁽⁸⁰⁾ Si riferiscono a neurodiritti M. IENCA, R. ANDORNO, *Verso nuovi diritti umani nell'era delle neuroscienze e delle neurotecnologie*, Life Sciences, Society and Policy, 2017, 13, (1), pp. 5, più di recente, M. IENCA, *Neurodiritti, quali nuove tutele per la sfera mentale: tutti i nodi etico-giuridici*, 2021, in <https://www.agendadigitale.eu/cultura-digitale/neurodiritti-quali-nuove-tutele-per-la-sfera-mentale-tutti-i-nodi-etico-giuridici/>.

⁽⁸¹⁾ Le tre posizioni emerse in dottrina sono analizzate in S. LIGTHART, M. IENCA, G. MEYNEN ET AL. *Minding Rights: Mapping Ethical and Legal Foundations of 'Neuro-rights.'* Cambridge Quarterly of Healthcare Ethics. 2023, 32(4):461-481. doi:10.1017/S0963180123000245.

⁽⁸²⁾ *Ex multis*, M. IENCA, R. ANDORNO, *Towards new human rights in the age of neuroscience and neurotechnology*, cit., S. LIGTHART, T. DOUGLAS, C. BUBLITZ, T. KOIJMANS, G. MEYNEN, *Forensic brain-reading and mental privacy in European Human Rights Law: Foundations and challenges*. Neuroethics 2021;14(2):191-203.

⁽⁸³⁾ *Ex multis*, J.C. BUBLITZ, *Novel neurorights: From nonsense to substance*, Neuroethics 2022;15(1):7; O. POLLICINO, *Costituzionalismo, privacy e neurodiritti*, MediaLaws, 2021, p. 9 ss. <https://www.medialaws.eu/wp-content/uploads/2021/08/2-2021-Pollicino.pdf>.

precedenti, che tende a considerare sufficiente il concetto di “abuso” rispetto alle interpretazioni dei diritti fondamentali della persona sanciti dalle carte internazionali e costituzionali ⁽⁸⁴⁾.

Nello scenario internazione sono state pubblicate alcune iniziative e studi. Ad esempio, nel 2019 l’Organizzazione per la cooperazione e lo sviluppo economico (OECD) ha adottato una *Raccomandazione sull’innovazione responsabile nelle neurotecnologie* ⁽⁸⁵⁾ volta a definire *standard* di responsabilità al fine di preservare la centralità del cervello e delle funzioni cognitive, nel rispetto dei principi di dignità, autonomia, libertà di pensiero, di tutela dell’identità e della vita privata. In particolare, la raccomandazione ammonisce le istituzioni, aderenti o meno al documento, affinché si attivino per promuovere un atteggiamento responsabile verso l’uso di neurotecnologie per la salute, volto all’inclusività e alla protezione della persona sia come individuo che come appartenente ad un gruppo da manipolazioni e compromissioni dell’integrità, autonomia, rispetto della vita privata e principio di non discriminazione, sia nel breve che nel lungo periodo.

Nel 2021, il comitato internazionale di bioetica dell’UNESCO ha pubblicato un rapporto su etica e intelligenza artificiale, dedicando un paragrafo ai rischi specifici delle neurotecnologie, ammonendo gli Stati Membri affinché le questioni etico-giuridiche emergenti da sistemi basati su interfacce *brain-computer* siano prese in considerazione (e dunque valutate) al fine di preservare la dignità umana e l’autonomia ⁽⁸⁶⁾.

Nonostante l’avanzamento delle applicazioni e delle neurotecnologie e la portata globale del dibattito etico-giuridico in materia ⁽⁸⁷⁾,

⁽⁸⁴⁾ S. MICHALOWSKI, *Critical reflections on the need for a right to mental self-determination*, in A. von ARNAULD, K. DER DECKEN, M. SUSI (a cura di) *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric*, Cambridge: Cambridge University Press; 2020:404-12.

⁽⁸⁵⁾ OECD, *Recommendation on Responsible Innovation in Neurotechnology*, <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>.

⁽⁸⁶⁾ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021, <https://unesdoc.unesco.org/ark:/48223/pf0000381137.page=37>, para 126.

⁽⁸⁷⁾ NS. JECKER - A. KO (2023). *Are Neurorights Global?* *AJOB Neuroscience*, 14(4), 369-371. <https://doi.org/10.1080/21507740.2023.2257151>, riferendosi alla posizione legata alla tutela della diversità culturale neurocognitiva, come elemento mancante tra diritti fondamentali della persona e contesto sociale promossa da K. HERRERA-FERRÁ, JM MUÑOZ, H. NICOLINI, G. SARUWATARI G. ZAVALA, V.M. MARTÍNEZ BULLÉ GOYRI

solo in Cile si è proceduto a statuire la protezione dell'attività cerebrale e dei dati da essa generati a fronte dell'avanzamento delle frontiere scientifiche e tecnologiche nella carta costituzionale ⁽⁸⁸⁾. La riforma cilena ha consentito alla Corte Suprema di Giustizia di affermare alcuni principi applicativi ⁽⁸⁹⁾. In particolare, nell'ambito di una sperimentazione, è stato confermato che i dati neurologici raccolti da un dispositivo *wireless* basato sull'elettroencefalografia non saranno mai “sufficientemente anonimi”, parafrasando la formula del considerando 26 GDPR, sebbene non applicabile alla fattispecie cilena in esame per ovvie ragioni di territorialità. Gli stessi, infatti, includono dettagli sulla gestualità e movimenti, tempi di reazione, attitudini e comportamenti da ricondursi all'attività cognitiva del cervello dell'utente; pertanto, si tratta di informazioni pseudonimizzate e non anonime, in quanto attraverso l'associazione con ulteriori dati, sicuramente in possesso del centro clinico, ma altresì rinvenibili da altre fonti, sarà sempre possibile per il titolare del trattamento, nella specie un'azienda privata, reidentificare il paziente — soggetto interes-

(2023). *Contextual and Cultural Perspectives on Neurorights: Reflections Toward an International Consensus*. *AJOB Neuroscience*, 14(4), 360-368. <https://doi.org/10.1080/21507740.2022.2048722>.

(88) Ley 25 Oct. 2021, n. 21.383, *Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas*, aggiungendo all'art. 19 un parágrafo del seguente tenore: “*El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella*”, <https://www.bcn.cl/leychile/navegar?idNorma=1166983>. In dottrina, S. RUIZ ET AL., *Efectos Negativos En La Investigación y El Quehacer Médico En Chile de La Ley 20.584 y La Ley de Neuroderechos En Discusión: La Urgente Necesidad de Aprender de Nuestros Errores*, *Revista medica de Chile* 149.3 (2021): 439-446.

(89) Corte Suprema di Giustizia del Cile, 9 agosto 2023, n. 1.080-2020, il caso riguarda un produttore di sistemi portatili di neuropotenziamento che utilizzano l'elettroencefalografia, offrendo neuro-cuffie, ovvero dispositivi wireless che funzionano come un auricolare con sensori che, tuttavia, raccolgono informazioni sull'attività elettrica del cervello (cioè dati neurologici), si vedano i contributi di B. RICARDO CAMARGO - N. RIED SOTO, *Neurociencia y derecho el impacto del neuroderecho en la práctica judicial chilena*, *Revista chilena de derecho* 48.3 (2022): 107-130 e di J.R. AGUILERA - N.W. SILVA (2023). *Neurodireitos, uma tentativa de proteção jurídicas das pessoas diante do uso de neurotecnologias*, *Revista De Direito Sanitário*, 23, e0014. <https://doi.org/10.11606/issn.2316-9044.rdisan.2023.194202>.

sato ⁽⁹⁰⁾. Alla luce di tali considerazioni, la Corte cilena ha specificato che tale trattamento avrebbe esposto l'utente ad una serie di ulteriori rischi, come l'eventuale accesso e riutilizzo (anche per diverse finalità, incluse quelle commerciali e di monitoraggio) non autorizzati a informazioni, non raccolte, ma generate dalle attività cerebrali. Ciò violerebbe i diritti fondamentali della persona, costituzionalmente tutelati all'art. 19 Cost. cilena. In particolare, sarebbe compromessa l'integrità psicofisica, che nel contesto specifico si manifesta attraverso la tutela del diritto alla *privacy* mentale e della libertà cognitiva dell'utente. La regolamentazione di tali "epifanie" di diritti fondamentali della persona spetta ad una legge di rango ordinario, attualmente ancora in forma di proposta presentata al senato cileno, e volta ad attuare il nuovo dettato costituzionale, stabilendo i requisiti e le condizioni per l'uso delle neurotecnologie ⁽⁹¹⁾.

Più che introdurre neurodiritti, il sistema cileno parrebbe aver identificato specifici rischi che le neurotecnologie determinano sui diritti fondamentali della persona: dignità, autonomia, integrità psicofisica, etc. il cui impatto è considerato talmente rilevante da meritare una copertura costituzionale in linea di principio e di rango primario per la relativa regolamentazione.

Applicando gli strumenti regolatori dell'UE al caso cileno si addi-viene alla medesima soluzione anche senza l'esplicita menzione dei rischi da neurotecnologie nelle normative di riferimento. Si potrebbe, infatti, rinvenire una violazione della dignità, laddove siano venute a mancare quelle misure tecnico-organizzative che i principi di trasparenza, equità, e *accountability* impongono allo sviluppatore e titolare del trattamento verso l'utente che, eventualmente, ignaro rispetto alla *governance* dei flussi di dati generati con il *device*, esprima un consenso non informato e — pertanto — invalido al trattamento. I neuro-dati, infatti, altro non sono che dati che espongono il titolare a particolari vulnerabilità e, come tali, possono rientrare nella categoria di dati

⁽⁹⁰⁾ M.I. CORNEJO-PLAZA, R. CIPPITANI, V. PASQUINO, *Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata*. Front Psychol. 2024 Feb 27;15:1330439. doi: 10.3389/fpsyg.2024.1330439.

⁽⁹¹⁾ Proyecto de ley, iniciado en moción de los Honorables Senadores señor Girardi, señora Goic, y señores Chahuán, Coloma y De Urresti, sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías, in *Boletín* 13828.19, <https://www.diarioconstitucional.cl/wp-content/uploads/2020/12/boletin-13828-19-nuroderechos.pdf>.

“sensibili”, nell’ambito di quelli relativi alla salute. A tal proposito, nel sistema europeo la base giuridica per il trattamento sarebbe regolamentata in seno all’art. 9 GDPR con riferimento alla natura dei dati e all’art. 22 GDPR relativamente alle attività di profilazione. Le valutazioni sulla supervisione di interfacce uomo-macchina e quelle sulla robustezza dei sistemi onde evitare accessi e usi non autorizzati sarebbero oggetto di analisi nell’ambito del Regolamento sull’IA ai sensi degli artt. 5 e 9, oltre che 50, come meglio spiegato nel Considerando 29.

Più che di nuovi diritti, dunque, occorre parlare di nuovi rischi cui si ricollegano, da un lato, la salute psico-fisica dell’individuo e, dall’altro, i valori democratici, che possono essere minati da distorsioni e manipolazioni artificiali della realtà. In questo senso, si esprime anche un recentissimo studio del Parlamento Europeo ⁽⁹²⁾, che ammonisce a non creare categorie frastagliate di diritti fondamentali, mantenendo l’interpretazione dei diritti riconosciuti quanto più omnicomprensiva, ciò al fine di evitare l’emergere di lacune, per la cui copertura, peraltro, non si potrebbe applicare la giurisprudenza esistente.

7. La regolamentazione UE per lo sviluppo di sistemi IA affidabili.

Il rapporto tra la regolamentazione della società dell’informazione e quella in materia di innovazione tecnologica è molto stretto per due ragioni: la prima, di tipo tecnico, riguarda il fatto che l’innovazione tecnologica in gran parte, sebbene non in via esclusiva, si basa sull’elaborazione di dati; la seconda deriva da un fattore temporale, in quanto le iniziative sull’IA sono successive a quelle sulla protezione e circolazione dei flussi di dati non solo in Europa, ma — come vedremo — in tutte le famiglie giuridiche, il che definisce le interrelazioni e i meccanismi di priorità per i processi di conformità rispetto ai diversi quadri normativi.

Ciò premesso, dopo anni di gestazione, l’UE si è finalmente dotata di una legislazione per l’intelligenza artificiale ⁽⁹³⁾: nell’analizzare il nuovo Regolamento UE n. 2024/1689 ci concentreremo, dunque, sul

⁽⁹²⁾ EUROPEAN PARLIAMENT, *The protection of mental privacy in the area of neuroscience. Societal, legal and ethical challenges*, STOA, PE 757.807 - July 2024, [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU\(2024\)757807_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf).

⁽⁹³⁾ Regolamento Europeo, 13 giugno 2024, n. 1689, cit.

verificare se l'approccio orientato alla tutela e promozione dei diritti dei bambini (osservato con l'approvazione del DSA) sia mantenuto, ovvero se le vulnerabilità degli utenti siano articolate come mero elemento di rischio da mitigare ai fini di ottenere un livello certo e accettabile di affidabilità del sistema. Per analizzare la portata della questione sottesa al ruolo della vulnerabilità nella nuova normativa, occorre fare un passo indietro.

Come accennato nelle premesse, al fine di preservare e promuovere i valori dell'Unione Europea, ancor prima dell'approvazione del Regolamento sull'IA, era stato formato un gruppo di lavoro composto da esperti interdisciplinari (il c.d. *High-Level Expert Group on Artificial Intelligence*), volto a tracciare i requisiti per orientare gli operatori economici a progettare e sviluppare sistemi che fossero eticamente accettabili e conformi al quadro giuridico esistente in una prospettiva umano-centrica ⁽⁹⁴⁾. Come risultato del gruppo di lavoro è stata pubblicata una *checklist* — la c.d. *Assessment List on Trustworthy Artificial Intelligence* (di seguito anche "ALTAI") del 2020 — composta di sette requisiti, la cui soddisfazione richiede(va) di analizzare le implicazioni mediante una linea guida composta di sessantatre domande volte a organizzare la valutazione sui diversi profili di criticità che un sistema può rappresentare per la tutela e promozione dei diritti fondamentali dell'utente o dell'utilizzatore, considerato sia come singolo, che come esponente di un gruppo di persone ⁽⁹⁵⁾. Tali linee guida sono state elaborate allo scopo di indirizzare la conformità etico giuridica sin dalla progettazione dei sistemi a perseguire una visione transdisciplinare, capace di porre la promozione dell'essere umano e dei relativi diritti fondamentali al centro dell'innovazione tecnologica, attraverso un percorso guidato che consideri anche le esigenze di

⁽⁹⁴⁾ C. RADCLYDE, M. RIBEIRO, RH. WORTHAM (2023), *The assessment list for trustworthy artificial intelligence: A review and recommendations*, in *Front. Artif. Intel.* 6:1020592, doi: 10.3389/frai.2023.1020.

⁽⁹⁵⁾ HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG), *Assessment List for Trustworthy Artificial Intelligence*, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342. I sette requisiti per soddisfare le esigenze di liceità, eticità e robustezza sono: 1) human agency and oversight, 2) technical robustness and safety, 3) privacy and data governance, 4) transparency 5) diversity, non-discrimination and fairness 6) environmental and societal well-being and 7) accountability. Sul rapporto tra i diversi requisiti: G. COMANDÉ, *Unfolding the Legal Component of Trustworthy AI: A Must to Avoid Ethics Washing*, in *Annuario di Diritto Comparato e di Studi Legislativi*, 2020, p. 29 s.

robustezza tecnica dei meccanismi di protezione dei flussi e dei processi decisionali automatizzati.

Ciò che richiede(va) l'ALTAI *checklist* è (era) di sviscerare contemporaneamente le problematiche che potrebbero (avrebbero potuto) far emergere tensioni tra la distribuzione e l'utilizzo di un determinato sistema con certe caratteristiche rispetto alla protezione e promozione dei diritti fondamentali della persona. L'esercizio di valutazione appare in parte confluito nei requisiti richiesti nella gestione della qualità del sistema di IA "ad alto rischio" e in parte tradotto nella c.d. FRIA (*Fundamental Rights Impact Assessment*) prevista dall'art. 27 del nuovo Regolamento ⁽⁹⁶⁾.

Tra i limiti operativi osservati rispetto all'ALTAI *checklist* emergeva in primo luogo l'ampiezza e dispersività di una delle prime questioni da analizzare: l'impatto sui diritti fondamentali della persona, che richiede(va) una sensibilità giuridica particolarmente orientata alla transdisciplinarietà per consentire l'identificazione e la misurazione dei rischi di compromissione e relativa mitigazione.

Il Regolamento sull'IA ha colto la centralità della questione dell'impatto sui diritti fondamentali della persona, mantenendo l'approccio *by design* e *by default* basato sulla valutazione dei rischi e volto a introdurre misure di sicurezza di tipo tecnico per raggiungere un accettabile grado di affidabilità per i sistemi cc.dd. ad alto rischio. La nuova legislazione, infatti, predetermina sulla base delle caratteristiche del sistema di IA in questione, l'appartenenza dello stesso ad una certa categoria di rischio, adeguando le attività di conformità etico-giuridica alle effettive necessità ⁽⁹⁷⁾. Numerosi sono i richiami alla legislazione di settore (dal GDPR, al DSA, al DMA, etc., ma non solo) al fine di ribadire che sviluppatori, utilizzatori (*deployer*) e distributori di sistemi di IA — a seconda del ruolo e delle responsabilità che si sono assunti — devono, in ogni caso, garantire l'adempimento alle obbligazioni relative alle attività che insistono sull'ecosistema della soluzione in questione. Ciò anche in ragione della funzione di raccordo rispetto alle

⁽⁹⁶⁾ A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, Volume 54, 2024, 106020, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2024.106020>.

⁽⁹⁷⁾ M. EBERS, *Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act* (June 19, 2024), available at SSRN: <https://ssrn.com/abstract=4870387> or <http://dx.doi.org/10.2139/ssrn.4870387>.

varie iniziative in materia di strategia europea dei dati che hanno consentito, attraverso interpretazioni sistematiche e analogiche, di colmare quelle lacune lasciate scoperte in fase di gestazione del nuovo regolamento, proteggendo i valori dell'UE in questi anni a fronte della rapida evoluzione delle tecnologie. In particolare, il Regolamento specifica che sono proibite quelle pratiche che si pongono in contrasto con la regolamentazione in materia di protezione dei dati personali, quella antidiscriminatoria, quella rivolta alla protezione del consumatore e del mercato ⁽⁹⁸⁾.

Per tale ragione, le pratiche di IA possono essere vietate (se incluse nell'elenco previsto dall'art. 5 del Regolamento), o essere considerate ad alto rischio (se previste nell'art. 6 o nell'Allegato III allo stesso) e, pertanto, richiedere dei requisiti di conformità che includono una valutazione e gestione dei rischi rispetto ai flussi di dati e alla relativa *governance*. Inoltre, relativamente alla robustezza tecnica dei sistemi, sono previste delle condizioni in ordine alla spiegabilità dei processi decisionali automatizzati e alla loro trasparenza al fine di evitare di incorrere o riprodurre *bias* ⁽⁹⁹⁾, ovvero di garantire precisione e accuratezza dei risultati desiderati nelle fasi di allenamento degli algoritmi e trattamento delle basi di dati.

Il Regolamento sull'IA riprende negli accennati articoli 9 e seguenti alcuni dei profili di valutazione elaborati nell'ALTAI *checklist*, introducendo — tuttavia — un sistema di gestione dei rischi volto ad avviare un monitoraggio costante incentrato sulla sussistenza, permanenza e aggiornamento delle condizioni di conformità durante il ciclo di vita ⁽¹⁰⁰⁾. Ciò al fine di assicurare l'aderenza ai valori condivisi in un

⁽⁹⁸⁾ Considerando 29.

⁽⁹⁹⁾ Molteplici significati vengono attribuiti al concetto di *bias*, che se associato ad un sistema algoritmico indica una deviazione del processo decisionale derivante da una scarsa o limitata accuratezza del sistema, vuoi per le modalità con cui è stato disegnato o per la natura dei dati con cui è stato allenato, che produce errori o effetti inappropriati o discriminatori per i soggetti interessati, v. A. DAVOLA, *Bias*, in G. COMANDÉ, *Elgar Encyclopedia of Law and Data Science*, cit., p. 60 ss.

⁽¹⁰⁰⁾ L'elenco dei sistemi ad alto rischio sono quelli enucleati nell'allegato III, che include quelli di identificazione biometrica remota, destinati a essere utilizzati per la categorizzazione biometrica, o di riconoscimento delle emozioni; quelli che sono destinati a fungere da componente di sicurezza per servizi essenziali o di interesse pubblico, quelli destinati alla gestione dei servizi educazionali e di istruzione, nei rapporti tra datore di lavoro e dipendente, nella gestione dei flussi migratori e richiedenti asilo, nella giustizia o nell'amministrazione dei processi democratici. J.

determinato momento storico, che dovrà essere provata attraverso una valutazione positiva delle implicazioni della tecnologia sviluppata sui principi di inclusività e non discriminazione, di equità, nonché sulla tutela dell'ambiente — intesa in termini di sostenibilità ecologica — e sul benessere sociale. Quest'ultimo profilo rileva in particolare in termini di possibilità di investigare il miglior modo non solo per introdurre il sistema sul mercato, ma anche per garantirne un uso appropriato, capace di sfruttare le potenzialità e opportunità dei processi decisionali automatizzati al fine ultimo di avanzare le frontiere della conoscenza e del progresso. In questo quadro, un profilo particolarmente rilevante è quello relativo all'accettabilità sociale nei processi organizzativi, economici o industriali di quella data tecnologia, vuoi perché sostitutiva di manodopera, vuoi per la necessità di mitigare atteggiamenti di iperfiducia o refrattari alla stessa.

Allo stesso tempo, si dovranno introdurre le misure tecnico-organizzative che, sulla base della normativa derivante dalla strategia europea dei dati, assicurino la conformità ai principi di protezione dei flussi rispetto ai profili di confidenzialità, integrità e disponibilità, specie laddove si tratti di informazioni personali, dando rilievo ai meccanismi per garantire la resilienza, tracciabilità e — più in generale — delle misure volte a garantire la *cybersicurezza* ⁽¹⁰¹⁾.

Con riferimento al governo dei dati, ad esempio, l'art. 10 del Regolamento sull'IA, richiamando la preventiva conformità alla normativa di settore esistente ⁽¹⁰²⁾, impone la verifica delle basi di dati relativamente agli otto indici volti a introdurre pratiche sia nelle fasi di addestramento, test, e convalida dei meccanismi ⁽¹⁰³⁾ e una analisi

SCHUETT, *Risk Management in the Artificial Intelligence Act*, in *European Journal of Risk Regulation*, 2023:1-19. doi:10.1017/err.2023.1.

⁽¹⁰¹⁾ J. VOSTOUPAL, V. STUPKA, J. HARAŠTA, F. KASL, PAVEL LOUTOCKÝ, K. MALINKA, *The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond*, in *Computer Law & Security Review*, Volume 53, 2024, 105988, <https://doi.org/10.1016/j.clsr.2024.105988>.

⁽¹⁰²⁾ In particolare, al GDPR, e al Regolamento UE n. 2018/1725 sul trattamento e la circolazione dei dati personali da parte di istituzioni, organi e organismi UE e della direttiva UE n. 2016/680 sui trattamenti dei dati personali in materia penale.

⁽¹⁰³⁾ Le pratiche sono elencate dalla lett. *sub a*) alla lett. *sub b*) e riguardano la necessità che la valutazione sia effettivamente atta a responsabilizzare lo sviluppatore rispetto alle scelte progettuali e alla formulazione di ipotesi, cui conseguentemente devono essere legati alla verifica della *compliance* nelle operazioni di trattamento dalla raccolta alla preparazione dei dati anche per esaminarne l'adeguatezza rispetto alle

rispetto alle possibili carenze (di qualità, quantità, rappresentanza geografica o funzionale) dei *set* per le finalità previste ⁽¹⁰⁴⁾. Il requisito della rendicontazione — *accountability* — appare declinato nei successivi artt. 11 e 12, rispettivamente sulla documentazione tecnica e sulla conservazione delle registrazioni, che introducono obblighi di tenuta e aggiornamento della documentazione rilevante e dei *log*, anche a fini di tracciabilità del funzionamento del sistema ⁽¹⁰⁵⁾. L'art. 13 si occupa, invece, della trasparenza, intesa sia in senso di misura organizzativa da associarsi al diritto all'informazione dell'utente, sia in ottica di spiegabilità dei meccanismi decisionali automatizzati. Mentre l'art. 14 riguarda il delicato profilo dell'interazione persona-macchina e della prevalenza della prima in termini di controllo e supervisione, obiettivo raggiungibile attraverso misure che consentano all'utente-supervisore di comprendere correttamente capacità e limiti del sistema in modo da poter responsabilmente intervenire in caso di non corretto funzionamento, evitando di incorrere in condotte di eccessiva fiducia nel risultato del processo automatizzato e favorendo l'utilizzo di strumenti propri per interpretarne gli esiti. Questo aspetto richiama il requisito che nell'ALTAI era identificato nello "*human oversight*", invitando lo sviluppatore ad adottare procedure per assicurare lo sviluppo di protocolli metodologici affinché la persona umana, acquisite competenze di supervisione della macchina, possa mantenere il controllo sulla stessa, nonché garantendo che i relativi diritti fondamentali costituiscano priorità rispetto alle esigenze tecniche di sviluppo e a quelle organizzative di utilizzo della data soluzione basata sull'IA.

Sino ad ora le raccomandazioni dell'ALTAI hanno guidato meccanismi di adeguamento spontaneo degli sviluppatori, oltre che la ricerca scientifica pubblica, in quanto la conformità ai valori etico-giuridici è stata recepita come contrattualmente obbligatoria per acce-

attività da far espletare e le possibili distorsioni e *bias* ovvero carenze o lacune da colmare dal punto di vista tecnico. I. CARNAT, *Addressing the Risks of Generative AI for the Judiciary: The Accountability Framework(s) Under the EU AI Act*, in *Computer Law and Security Review*, 2024, <https://doi.org/10.1016/j.clsr.2024.106067>.

⁽¹⁰⁴⁾ P. FRIEDL, G.G. GASIOLA, *Examining the EU's Artificial Intelligence Act*, *VerfBlog*, 2024/2/07, <https://verfassungsblog.de/examining-the-eus-artificial-intelligence-act>.

⁽¹⁰⁵⁾ C. NECATI PEHLIVAN, N. FORGÓ, P. VALCKE, *The EU Artificial Intelligence (AI) Act: A Commentary*, Kluwer Law International, 2024.

dere ai finanziamenti pubblici europei e anche nazionali ⁽¹⁰⁶⁾. Ciò ha promosso un atteggiamento di responsabilizzazione degli operatori economici e degli attori coinvolti verso l'introduzione nei cicli di produzione di soluzioni basate sull'IA di momenti dedicati alla valutazione dei rischi e conseguente presa di coscienza e accettazione delle implicazioni di scelte tecniche e organizzative volte a mitigare l'occorrenza e la serietà del pregiudizio all'eventuale verificarsi del fattore previamente identificato. Altro pregio dell'ALTAI è stato quello di sensibilizzare alla preservazione e promozione di un ruolo attivo all'essere umano nei processi di addestramento, test e validazione degli algoritmi: spetta, infatti, all'operatore umano intervenire per ripristinare eventuali errori, sbilanciamenti o conseguenze che si rendano non accettabili dal punto di vista etico, giuridico e della robustezza, direttamente nell'ambito del processo automatizzato ⁽¹⁰⁷⁾.

Dalla combinazione di questi elementi prende forma il concetto di cultura digitale e alfabetizzazione che, da un lato, mira a svolgere una funzione sociale, mediante una “*diffusione informata dei sistemi di IA*” rispetto alle opportunità, ai rischi e ai possibili danni che gli stessi possono causare come missione e, dall'altro lato, a garantirne l'attuazione tra gli operatori economici, prevedendo l'obbligo per i *provider* e i *deployer* di adottare misure per garantirne “*nella misura del possibile un livello sufficiente*” di istruzione e formazione per il personale. In particolare, l'art. 4 del Regolamento sull'IA esplicita che la diligenza rispetto all'adempimento degli obblighi formativi deve prendere in considerazione le conoscenze tecniche, l'esperienza, il livello di istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati dal personale dedicato, ma non solo. Occorre, infatti, che sia prestata attenzione agli utenti, sia come singoli che come appartenenti a gruppi. Il che significa soffermarsi ad analizzare la posizione dei minori di età, quali utenti vulnerabili, considerando il livello di alfabetizzazione ed educazione digitale nella progettazione e

⁽¹⁰⁶⁾ I programmi di finanziamento della Commissione Europea, come H2020, Horizon Europe, European Research Council, richiedono da diversi anni sia lo svolgimento di un *self-assessment* etico e giuridico, sia un monitoraggio durante l'intero ciclo di vita del progetto attraverso anche attività di reportistica ed eventuale nomina di esperti o di commissioni per fornire elementi di indirizzo.

⁽¹⁰⁷⁾ B. GREEN, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, in *Computer Law & Security Review*, Volume 45, 2022, <https://doi.org/10.1016/j.clsr.2022.105681>.

sviluppo di sistemi che siano a loro destinati, nonché pensare alla possibilità che gli stessi sistemi possano (o debbano), a seconda delle specifiche tecniche e delle funzioni, essere utilizzate da familiari, o educatori, o adulti che più in generale si prendono cura del minore durante l'uso ⁽¹⁰⁸⁾.

È dato di fatto, inoltre, che il progresso scientifico-tecnologico non abbia atteso il legislatore europeo per irrompere sul mercato (anche europeo), evolvendo quotidianamente per qualità e quantità di prestazioni ottenibili a mezzo di processi decisionali automatizzati e incrementando i possibili campi di applicazione. È altrettanto palese, inoltre, che l'IA nasce ed opera attraverso trattamenti di dati personali (e non) e che, pertanto, il vuoto normativo ben possa trovare nei principi informatori esplicitati nella normativa di settore bussole orientative al fine di dedurre le modalità con cui proteggere e promuovere i diritti fondamentali della persona nello scenario non (ancora) regolamentato. Nelle more dell'attuazione del Regolamento sull'IA, peraltro, le grandi aziende hanno aderito all'iniziativa della Commissione Europea chiamata Patto sull'IA, volta ad accompagnarle nel volontario processo di adeguamento anticipato rispetto ai termini normativi anche attraverso percorsi formativi e di alfabetizzazione indispensabili per poter valutare e mitigare i sistemi cc.dd. ad alto rischio ⁽¹⁰⁹⁾. Questi ultimi, a differenza di quelli classificati come “*rischio inaccettabile*”, che sono vietati, sono quelli che trattano dati di natura sensibile (come dati biometrici, sanitari, giudiziari etc.) utilizzati in settori particolarmente critici rispetto alle vulnerabilità umane: educazione, sanità, trasporto, rapporto di lavoro, giustizia etc. e che, pertanto, richiedono l'adempimento di una serie di obblighi per essere considerati accettabili. In questi casi i sistemi di IA devono soddisfare i requisiti di conformità attuando un sistema di gestione della qualità che consenta il monitoraggio dell'efficacia delle misure tecnico-organizzative implementate a mitigazione dei rischi individuati in ogni fase del ciclo di vita di progettazione,

⁽¹⁰⁸⁾ K. STOLPE, J. HALLSTRÖM, *Artificial intelligence literacy for technology education*, in *Computers and Education Open*, Volume 6, 2024, 100159, ISSN 2666-5573, <https://doi.org/10.1016/j.caeo.2024.100159>.

⁽¹⁰⁹⁾ G. FINOCCHIARO, *La proposta di Regolamento sull'Intelligenza Artificiale: il modello Europeo basato sulla gestione del rischio*, *Dir. Informazione e dell'informatica*, 2022, p. 303 ss. A. MANTELERO - M. S. ESPOSITO, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer Law & Security Review*, Volume 41, 2021, 105561, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2021.105561>.

sviluppo e validazione degli stessi. Una volta immessi sul mercato, prima del loro utilizzo nelle pubbliche amministrazioni o in enti privati che forniscono servizi pubblici, i relativi *deployer* devono non solo effettuare una analisi delle implicazioni sui diritti fondamentali degli utenti — c.d. FRIA — ma anche notificarne i risultati all'organismo di vigilanza del mercato.

Questo duplice meccanismo di conformità etico-giuridica per i sistemi ad alto rischio consente di separare l'analisi sull'affidabilità del sistema di per sé per come disegnato e progettato, da quella relativa alle ricadute nello specifico scenario ove la tecnologia deve poter essere introdotta in una macchina organizzativa con caratteristiche tecniche e risorse umane proprie.

Come per la strategia europea dei dati, infatti, l'approccio adottato dal legislatore UE per regolamentare l'IA è diretto a individuare obblighi per gli operatori attraverso la definizione di un paradigma di responsabilizzazione, oltre che di responsabilità, basato sulla valutazione del rischio da effettuare caso per caso al fine di implementare idonee misure capaci di mitigare, sino a rendere accettabile, se non annullare, le possibili esposizioni dell'utente a compromissioni, violazioni e intrusioni rispetto ai diritti fondamentali della persona, sia come singolo, sia come appartenente ad una particolare categoria di soggetti ⁽¹¹⁰⁾.

Per effettuare la valutazione degli impatti che le capacità di “*fare inferenze*” di un sistema basato sull'IA può produrre sul singolo e sulla società, occorre analizzare non solo la specifica soluzione, ma anche gli scenari e i settori applicativi. Uno stesso sistema, infatti, può ottenere risultati, costruire modelli e/o algoritmi a partire da dati generali o sensibili, che possono influenzare una circostanza fisica o digitale in maniera diversificata, secondo livelli progressivi di autonomia ⁽¹¹¹⁾. Predizioni e nuovi contenuti possono assumere, peraltro, ruoli di raccomandazione o di decisione a seconda dell'accuratezza e potenzia-

⁽¹¹⁰⁾ Il Considerando 4 riassume l'essenza del dibattito interdisciplinare della materia, specificando che, a seconda delle circostanze e, in particolare, dell'ambito di applicazione della soluzione, del reativo uso e dello stato di avanzamento della tecnologia adottata, l'IA può generare rischi ed esporre l'individuo a pregiudizi per i diritti fondamentali della persona ovvero per gli interessi pubblici regolati dall'UE; il Considerando 14 giustifica l'adozione del sistema basato sulla valutazione del rischio al fine di individuare norme efficaci e proporzionate anche in ragione dei sette requisiti identificati dall'High Level Group on Trustworthy AI, nell'ambito dell'ALTAI *checklist*.

⁽¹¹¹⁾ Considerando 6.

lità del sistema, incidendo in misura più o meno significativa sul processo decisionale.

Per tale ragione, sin dai *consideranda* del nuovo Regolamento si distinguono specifici divieti di sviluppo di tecniche basate sull'IA ⁽¹¹²⁾. Ad esempio, vi rientrano quelle di manipolazione dei comportamenti che sono classificate come abusi delle potenzialità dell'IA rispetto all'autonomia delle persone ⁽¹¹³⁾. A tal proposito, sono richiamati quegli elementi che assumono una pluralità di forme (da stimoli audiovisivi a componenti che vanno oltre la percezione umana), perseguendo lo scopo di *“sovertire o diminuire l'autonomia delle persone, la capacità decisionale e di compiere libere scelte”*, senza che ne siano a conoscenza o consapevoli. In questo contesto, sono menzionate le interfacce neurali (*machine-brain interfaces*) o le applicazioni che sviluppino realtà virtuali come sistemi di IA, che non possono essere messe sul mercato o utilizzate se hanno come oggetto (o come ragionevole effetto) quello di causare pregiudizi a singoli o a categorie di persone ⁽¹¹⁴⁾. Diversamente, la messa sul mercato degli stessi è consentita, laddove l'utilizzo di queste pratiche sia giustificato da idonea base giuridica, come ad esempio il consenso dell'utente, e siano perseguiti scopi terapeutici o riabilitativi, seguendo gli *standard* clinici e le condizioni dettate dalla normativa di settore ⁽¹¹⁵⁾.

⁽¹¹²⁾ Il Considerando 133 si riferisce a *“varietà di sistemi di IA”*, mentre i *consideranda* 4 e 138 parlano di *“famiglie di tecnologie”*, dal punto di vista tecnico, H. ABBASS, *Editorial: What is Artificial Intelligence?*, in *IEEE Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 94-95, April 2021, doi: 10.1109/TAI.2021.3096243.

⁽¹¹³⁾ Il Considerando 29 evidenzia gli impatti negativi delle tecniche manipolative rispetto alla salute psicofisica e rispetto alla sfera economica del soggetto. Sul concetto di manipolazione, si veda la ricostruzione di M. IENCA, *On Artificial Intelligence and Manipulation*. *Topoi* 42, 833-842 (2023). <https://doi.org/10.1007/s11245-023-09940-3>.

⁽¹¹⁴⁾ Sempre il Considerando 29 richiama peraltro la direttiva sulle pratiche commerciali scorrette, Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio (« direttiva sulle pratiche commerciali sleali ») (GU L 149 dell'11.6.2005, pag. 22).

⁽¹¹⁵⁾ Communication to the Commission Approval of the content of the draft Communication from the Commission - Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), in particolare p. 80.

Ulteriori divieti sono previsti per sistemi che inferiscono emozioni, per diverse ragioni: da un lato, l'emozione è un concetto che varia a seconda delle circostanze e del contesto socio-culturale ⁽¹¹⁶⁾; dall'altro, laddove messi sul mercato, si tratterebbe di sistemi scarsamente affidabili per mancanza di specificità e limitata capacità di astrarre e generalizzare, forieri — dunque — di possibili effetti discriminatori, nonché di intrusioni ingiustificate nella sfera intima della persona. Ciò è particolarmente vero negli ambienti di lavoro e nel settore educativo, in ragione dello squilibrio tra le posizioni rispettivamente di datore di lavoro e lavoratore e di docente e discente che espone la persona a possibili distorsioni che impattano eccessivamente sulla realizzazione dei diritti fondamentali, come vedremo in seguito, soprattutto con riferimento all'istruzione e formazione in ragione della prossimità degli scenari e delle possibili soluzioni rispetto alle esigenze dei minori di età ⁽¹¹⁷⁾, mentre con riferimento agli usi terapeutici, in contesti clinici o di sicurezza, con le dovute misure di salvaguardia, anche tali sistemi sono da ritenersi accettabili, in ragione delle finalità perseguite ⁽¹¹⁸⁾. A questo ultimo proposito, un altro elemento rilevante per le valutazioni di impatto è la possibilità di consentire agli utenti in qualsiasi momento di non utilizzare il processo decisionale automatizzato, ovvero di intervenire durante l'elaborazione, controllandola manualmente, senza che ciò produca conseguenze sull'effetto finale dell'operazione ⁽¹¹⁹⁾.

Infine, la parte legata alla robustezza tecnica è affrontata dall'art. 15 che riguarda le misure per la gestione della vulnerabilità tecnica o malfunzionamento dei sistemi di IA e richiama l'applicazione di *standard* riconosciuti ⁽¹²⁰⁾.

⁽¹¹⁶⁾ Sia concesso rinviare a D. AMRAM, *Pecunia doloris: (ap)prezzare il dolore. Il ruolo delle emozioni e dei sentimenti nella responsabilità civile*, in *Riv. it. med. leg.*, 2021, 2, 491.

⁽¹¹⁷⁾ *Infra*, Cap. III.

⁽¹¹⁸⁾ K.K. SMITH, V. BLANES-VIDAL, E.S. NADIMI, U. RAJENDRA ACHARYA, *Emotion recognition and artificial intelligence: A systematic review (2014-2023) and research recommendations*, in *Information Fusion*, Volume 102, 2024, 102019, ISSN 1566-2535, <https://doi.org/10.1016/j.inffus.2023.102019>.

⁽¹¹⁹⁾ R. RODRIGUES, *Legal and human rights issues of AI: Gaps, challenges and vulnerabilities*, *Journal of Responsible Technology*, Volume 4, 2020, 100005, ISSN 2666-6596, <https://doi.org/10.1016/j.jrt.2020.100005>.

⁽¹²⁰⁾ J. SOLER GARRIDO, D. FANO YELA, C. PANIGUTTI, H. JUNKLEWITZ, R. HAMON, T. EVAS, A. ANDRÉ, S. SCALZO, *Analysis of the preliminary AI standardisation work plan in support of the AI Act*, EUR 31518 EN, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/5847, JRC132833; A. TARTARO, *Regulating by stan-*

Questo breve *excursus* è funzionale a comprendere la complessità e la pluralità dei profili di analisi che gli sviluppatori di sistemi di intelligenza artificiale devono prendere in considerazione per la tutela degli utenti minori di età e consente di far emergere i problemi pratici collegati alla necessità di integrare l'approccio basato sulla valutazione del rischio rivolto agli operatori economici con lo sviluppo di conoscenze e competenze specifiche che possano rendere l'utente responsabile e, dunque, meno vulnerabile.

7.1. (Segue). *L'intelligenza artificiale a portata dei minori di età: i lavori dell'UE e del Consiglio d'Europa a partire dalle raccomandazioni elaborate dall'UNICEF.*

Le osservazioni generali, così come le valutazioni di impatto, necessitano di “*accomodamenti ragionevoli*” ⁽¹²¹⁾ per indirizzare i profili di criticità emergenti rispetto alle categorie di soggetti vulnerabili.

Sin dall'inizio del dibattito sull'IA, ad esempio, è apparso necessario riflettere sull'opportunità di introdurre specifici profili a misura di bambino. I sistemi di IA attualmente sul mercato sono, infatti, in gran parte progettati senza considerare né i punti di vista dei diritti dei bambini, né l'impatto che il relativo utilizzo può avere sul loro benessere e sviluppo, che è spesso ignoto agli operatori economici ⁽¹²²⁾.

Per ovviare a tale lacuna, dapprima l'UNICEF ha elaborato nel 2021 delle *policy* per guidare la valutazione di impatto dei sistemi di IA, utilizzando come chiave di lettura la lente dei diritti dei bambini, attraverso l'applicazione di nove requisiti che — vedremo — adottano una duplice prospettiva di protezione e di promozione ⁽¹²³⁾. Mentre il Consiglio d'Europa (di seguito anche “CoE”) ha lanciato una “*Strategia per i diritti del fanciullo (2022-2027)*”, pubblicando uno studio sulle implicazioni emergenti dall'assenza di previsioni normative che affron-

dards: current progress and main challenges in the standardisation of Artificial Intelligence in support of the AI Act, in *European Journal of Privacy Law and Technologies*, 2023, <https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1792/1349>.

⁽¹²¹⁾ G. COMANDÉ, *cit.*

⁽¹²²⁾ COUNCIL OF EUROPE, *Proposals for a CDENF Report on the Rights of the Child and Artificial Intelligence*, 2022, <https://rm.coe.int/cdenf-2022-20rev-concept-note-rc-and-ai-revised-/1680a8791e>.

⁽¹²³⁾ UNICEF, *Policy guidance on AI for children*, 2021, in <https://www.unicef.org/globalinsight/media/2356/file/UNICEF-Global-Insight-policy-guidance-AI-children-2.0-2021.pdf>.

tino la tutela e la promozione dei diritti dei bambini nel contesto dell'IA.

I due documenti rispondono ad esigenze analoghe, ma affrontano la criticità con approcci diversificati. Le raccomandazioni UNICEF sono rivolte a tutti gli operatori e soggetti interessati, istituzionali o privati, al fine di promuovere alcuni requisiti che, se implementati nel ciclo della progettazione e sviluppo delle applicazioni, sono capaci di assecondare le esigenze dei minori di età con funzionalità specifiche. Mentre la Strategia CoE si occupa di sensibilizzare gli Stati Membri ad attivare percorsi legislativi dell'IA che pongano attenzione sui rischi e sull'opportunità dell'uso delle nuove tecnologie da parte dei minori di età. Parallelamente i lavori del Comitato sull'Intelligenza Artificiale insediato presso il CoE hanno portato nel 2024 alla pubblicazione di una Convenzione quadro sull'intelligenza artificiale, diritti umani, democrazia e *rule of law*, che dedica l'art. 18 alle misure per i soggetti vulnerabili (disabili e minori di età) ⁽¹²⁴⁾.

In questo contesto, analizzando nel dettaglio i relativi contenuti, notiamo che i lavori dell'UNICEF si pongono come strumento interpretativo capace di valorizzare il ruolo ermeneutico che la Convenzione ONU ha rispetto alla giurisprudenza della Corte di Strasburgo ⁽¹²⁵⁾ e alla Corte di Lussemburgo ⁽¹²⁶⁾. Complice il fatto che tutti gli Stati

⁽¹²⁴⁾ COUNCIL OF EUROPE, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, 17 maggio 2024, <https://rm.coe.int/1680afae3c>.

⁽¹²⁵⁾ E. CANNIZZARO, *Diritto internazionale*, Giappichelli, 2018, p. 232 ss.; K. GAVRYSH, *Lo stato di emergenza e la dottrina del vacuum nella prassi della Corte europea dei diritti dell'uomo*, in *Rivista di diritto internazionale*, 2019, pp. 79-107, p. 86 ss. In giurisprudenza, *ex multis*: Corte EDU, sentenza del 15 settembre 2011, Schneider c. Germania (n. 17080/07), Corte EDU, sentenza del 23 ottobre 2018, Petrov e X c. Russia (n. 23608/16), Corte EDU, sentenza del 10 gennaio 2019, Wunderlich c. Germania (n. 18925/15).

⁽¹²⁶⁾ Come osserva la Fundamental Rights Agency, “la CGUE emette sempre più spesso sentenze riguardanti i diritti dei minori in vari ambiti, quali la libera circolazione, la cittadinanza dell'UE, la migrazione, l'affidamento, la residenza abituale, la vita familiare e la non discriminazione” *Ex multis*: CGUE, sentenza del 22 dicembre 2010, Joseba Andoni Aguirre Zarraga c. Simone Pelz, causa C-491/10 PPU, CGUE, 2019, SM c. Entry Clearance Officer, UK Visa Section, causa C-129/18, CGUE, 2014, E. c. B., causa C-436/13, CGUE, 2010, Barbara Mercredi c. Richard Chaffe, causa C-497/10 PPU. Sul dialogo fra le corti F. FONTANELLI, G. MARTINICO, P. CARROZZA (a cura di), *Shaping Rule of Law Through Dialogue. International and Supranational Experiences*, Groningen, 2009.

Membri del Consiglio d'Europa che sono anche parte dell'UE siano tutti parte della CRC, le linee guida UNICEF svolgono un ruolo ermeneutico rispetto alle riflessioni sulla tutela e promozione dei diritti dell'infanzia e dell'adolescenza che, nella specie, sono confluite anche nel Regolamento UE n. 1689/2024, ove si statuisce — seppur in termini più generici rispetto all'illustrato DSA — che i profili di rischio per la categoria dei minori di età (al pari di quelli emergenti per gli altri gruppi di soggetti vulnerabili) devono essere analizzati con metodi propri e adatti ad individuare specifiche misure di mitigazione degli stessi.

Per tale ragione, si può osservare come ciascun monito dell'UNICEF possa ispirare l'adozione di misure di salvaguardia — sia tecniche che organizzative — e costituire un parametro di valutazione rispetto all'attuazione degli obblighi per gli operatori.

La prima raccomandazione UNICEF riguarda la necessità che il sistema sia disegnato per supportare il benessere del minore, attraverso l'invito a sostenere lo sviluppo di ecosistemi atti a comprendere le esigenze poste alla base della crescita psicofisica e sociale dell'utente, quale adulto del domani. A questo proposito, si percepisce la necessità di differenziare gli interventi in ragione dell'età, del contesto socio-economico, e delle possibili ulteriori esigenze che possono caratterizzare l'utenza di uno specifico sistema. La raccomandazione fornisce a *provider*/sviluppatori/fornitori e *deployer* i profili da tenere in considerazione nella valutazione di impatto.

Il secondo e il terzo requisito (*i.e. Garantire l'inclusione dei bambini e per i bambini e Dare la priorità all'equità e alla non discriminazione dei bambini*), invece, si riferiscono alla necessità di perseguire l'obiettivo di raggiungere i più elevati gradi di inclusività, sia con riguardo all'accesso a tutti i bambini alle nuove tecnologie, sia relativamente alla necessità di instaurare processi virtuosi di co-partecipazione che coinvolgano gli stessi nella progettazione e sviluppo delle soluzioni anche al fine di evitare risultati forieri di discriminazioni. Anche in questo caso, la raccomandazione può essere utilizzata per definire in sede di interpretazione del Regolamento sull'IA alcuni livelli di diligenza: il coinvolgimento dei portatori di interessi nelle attività di progettazione, sviluppo, e test non solo non può escludere i minori di età, ma deve essere articolata in modo da dimostrare una rappresentazione delle possibili e diverse vulnerabilità che possono costituire barriere all'accesso inclusivo alla data soluzione.

Gli altri elementi delle linee guida UNICEF (*i.e. Proteggere i dati e la privacy dei bambini, Garantire la sicurezza per i bambini, Provvedere alla trasparenza, alla comprensibilità e alla responsabilità verso i bambini*), invece, riecheggiano gli illustrati requisiti etico-giuridici declinati nell'ALTAI *checklist*, identificando specifici elementi di valutazione rispetto alle vulnerabilità del soggetto minore di età. In particolare, con riferimento alla tutela dei dati e della riservatezza, l'UNICEF raccomanda di prendere in considerazione, tanto il singolo utente minore di età, quanto la pluralità di esposizione a pericoli conseguente a eventuali classificazioni prodotte dai processi algoritmici. Sulla sicurezza e robustezza, inoltre, l'attenzione si articola rispetto alle minacce *online* e ai pericoli derivanti da abusi e/o usi impropri del sistema, che espongano i minori di età a pericoli anche nella dimensione fisica. In questo senso, la dimensione digitale incrementa l'occorrenza di rischi noti anche nella dimensione fisica. Un "*adattamento*" specifico alle esigenze dei minori è infine richiesto anche con riferimento ai requisiti di trasparenza e spiegabilità rispetto alle specifiche vulnerabilità dei minori. In particolare, il linguaggio utilizzato per informare e spiegare i processi decisionali automatizzati deve poter essere comprensibile e alla portata dell'utente: pertanto meno tecnico e formale per certi aspetti, ma allo stesso tempo esaustivo per consentire non solo un effettivo esercizio dei diritti in qualità di utente di un certo sistema, ma anche per sensibilizzare ad evitare rischi d'esposizione che, invece, non impattano sull'adulto in quanto già maturo e, pertanto, non richiedono di essere specificamente indirizzati ⁽¹²⁷⁾. In questa prospettiva, l'uso della formula di richiamo ai "*diritti fondamentali dei minori*" presente nel Regolamento sull'IA, come nell'art. 9, identifica un insieme di posizioni da tutelare alla stregua di altri diritti fondamentali della persona, non perché i minorenni non debbano accedere ai meccanismi generali di tutela, in quanto persone, ma per sottolineare la peculiarità della condizione di incapacità del minore di età che richiede approfondimenti tecnici e organizzativi per soddisfare il requisito di *accountability*, che definisce la regola di diligenza nello scenario pratico.

Una maggiore consapevolezza tra gli operatori, sia istituzionali che privati, a prestare attenzione alle esigenze dei bambini e a perseguirne gli interessi superiori nello sviluppo, adozione e utilizzo di sistemi di IA

⁽¹²⁷⁾ J.M. ALONSO, *Explainable Artificial Intelligence for Kids*, in 11th Conference of the European Society for Fuzzy Logic and Technology (EUSFLAT 2019), doi: 10.2991/eusflat-19.2019.21.

presuppone, inoltre, un impegno a educare e formare gli utenti affinché sviluppino competenze specifiche per poter fruire dei servizi e prodotti digitali — e delle relative potenzialità — con maggiore cognizione di causa. Il richiamo alla sensibilizzazione e alfabetizzazione rispetto ai sistemi di IA destinati ai minori di età, da un lato, e il monito ad incentivare lo sviluppo di competenze specifiche per formare l'adulto di domani attraverso le nuove tecnologie, espressi nelle ultime due raccomandazioni UNICEF, si pongono, ancora una volta, in una posizione privilegiata per corroborare la necessità che sviluppatori, fornitori e *deployer* investano sull'alfabetizzazione e sulla formazione del personale. L'obiettivo comune è, infatti, che si formi una cultura responsabile dei dati e dell'innovazione volta a consentire di percepire al livello organizzativo e — dunque implementare *by design* e *by default* nelle applicazioni concrete — gli approfondimenti che non solo l'età anagrafica, ma anche le altre condizioni di vulnerabilità dell'utente possano essere riconosciute e propriamente indirizzate. In aggiunta, l'UNICEF invita tutti gli operatori — istituzionali o privati — a contribuire ad interventi che sviluppino specifiche competenze adatte a utilizzare consapevolmente le nuove tecnologie.

A tal proposito, si osserva che al Considerando 28 del Regolamento sull'IA è formulata una sorta di dichiarazione di intenti della Commissione Europea rispetto alle pratiche abusive e pregiudizievoli che possano manipolare, sfruttare e controllare socialmente gli utenti — come individui o come appartenenti a gruppi — ritenendole lesive dei valori dell'UE, inclusi i diritti dei minori e per tale ragione da proibirsi, nonostante i possibili e numerosi “*utilizzi benefici*”. Successivamente, il Considerando 48 indica nell'ambito di un elenco di diritti fondamentali della persona su cui un sistema ad alto rischio può impattare, la posizione dei bambini, quali soggetti vulnerabili, il cui benessere (e dunque non solo il non-nuocere) ⁽¹²⁸⁾ deve essere prioritariamente perseguito durante lo sviluppo, distribuzione e uso delle applicazioni.

(128) Per una riflessione recente si vedano i contributi di AA.VV., E. CECCHERINI - F. BRUNETTA D'USSEAUX (a cura di), *Best interest(s) of the child. Una delicata e controversa declinazione*, Editoriale Scientifica, 2023 e AA.VV., M. BIANCA (a cura di), *The best interest of the child*, Roma, 2021 letti in ragione degli elementi che caratterizzano oggi l'interpretazione del principio di interesse superiore del fanciullo, fornendo “*orientamenti concreti ma flessibili (...): i) opinioni del minore; ii) identità del minore; iii) tutela dell'ambiente familiare e mantenimento dei rapporti; iv) cura, protezione e sicurezza del minore; v) situazioni di vulnerabilità; vi) diritto alla salute; vii) diritto all'istruzione*”, F. ALBANO, *I best interests of the child tra passato, presente e*

In altri termini, il Regolamento sull'IA abbraccia l'approccio basato sulla valutazione del rischio secondo cui, accanto allo sfruttamento delle opportunità, occorre evitare che l'utente possa veder compromessi i propri diritti fondamentali (dalla dignità, alla vita privata e familiare, al diritto di associarsi, di esprimere un'opinione, alla presunzione di innocenza, al giusto processo, all'inclusività intesa come divieto di discriminazione e parità rispetto a possibili minoranze, sia come singolo che come appartenente a specifiche categorie di utenti, come i lavoratori, i consumatori, le persone con disabilità, etc). A questo meccanismo di identificazione, prevenzione e mitigazione dei rischi di esporre il singolo a pregiudizi si aggiunge la necessità di procedere a valutazioni specifiche, laddove il soggetto interessato dall'applicazione non abbia compiuto la maggiore età e sia, dunque, portatore di vulnerabilità connesse alla limitata capacità di discernimento. La normativa richiama sia l'art. 24 della Carta dei diritti fondamentali dell'UE, sia la Convenzione sui diritti dell'infanzia e dell'adolescenza, fornendo una base normativa di rango superiore per orientare le interpretazioni e gli sforzi sistematici sull'identificazione di meccanismi di valutazione e mitigazione degli impatti dei sistemi di IA sui minori. Tale tecnica legislativa non appare mossa dall'intento del legislatore dell'UE di tracciare confini tra categorie giuridiche, bensì, con approccio più pragmatico, verosimilmente, sembra guidata dall'intenzione di fornire esempi quanto più esaustivi, anche in risposta alle menzionate sollecitazioni dell'UNICEF, affinché una effettiva attenzione sia prestata dagli operatori economici al perseguimento degli interessi dei minori. Propendere per questa seconda interpretazione è funzionale alla responsabilizzazione degli operatori chiamati così a non poter eludere una valutazione sui diritti fondamentali dei bambini in termini di *accountability*, in quanto espressamente menzionati quali utenti finali vulnerabili.

A ben vedere, infatti, la valutazione di impatto appare essere promossa a più marce, con livelli di granularità differenziata: lo sviluppatore deve seguire, dapprima, una analisi dei rischi rispetto ai singoli diritti fondamentali della persona, per poi declinare i risultati con le lenti degli interessi superiori dei minori al fine di completare l'analisi senza tralasciare gli elementi distintivi della valutazione generale e al

futuro, ibidem, XXV. Si vedano anche i contributi di L. LENTI, *Note critiche in tema di interesse del minore*, in *Riv. dir. civ.*, 2016, p. 86, V. SCALISI, *Il superiore interesse del minore. Ovvero il fatto come diritto*, cit.

contempo perseguire con lenti “*adequate*” e “*adattate*” il benessere dei fanciulli ⁽¹²⁹⁾.

A questo proposito, il citato articolo 18 della Convenzione sull'intelligenza artificiale, diritti umani, democrazia e *rule of law* del CoE ⁽¹³⁰⁾ presta attenzione alle persone con disabilità e ai bambini, stabilendo che ciascuno Stato debba tenere in seria considerazione ogni specifico bisogno e vulnerabilità rispetto a queste due categorie di soggetti, in allineamento con quanto previsto dalla normativa nazionale, anche laddove le Convenzioni sulla disabilità e sui diritti dell'infanzia non siano state ratificate ⁽¹³¹⁾. Il CoE fornisce indicazioni sugli interventi necessari per l'implementazione dei principi espressi nell'art. 20 della stessa Convenzione, dove è promossa l'educazione digitale per la popolazione in generale, specificando nel documento di accompagnamento di riferirsi sia allo sviluppo di competenze tecniche, che alle conoscenze generali, rispetto ai rischi e all'impatto dei sistemi di IA sui profili etico-giuridici e sociali. Anche in questo contesto, peraltro, interventi che includano programmi di educazione o alfabetizzazione digitale si rendono particolarmente adatti, soprattutto se rivolti alle categorie di soggetti più deboli, come i bambini, gli anziani e i soggetti meno rappresentati nel contesto sociale di riferimento al fine di incrementare il livello di consapevolezza rispetto all'uso (e non solo allo sviluppo) delle nuove tecnologie. Lo stesso articolo 20 conv., inoltre, si esprime in termini di sviluppo di “*competenze specifiche ed esperte*” per coloro che sono responsabili della valutazione e mitigazione dei rischi dei diversi sistemi ⁽¹³²⁾, richiamando così il principio di alfabetizzazione espresso anche dal Regolamento sull'IA.

⁽¹²⁹⁾ Il perseguimento dell'interesse superiore del fanciullo costituisce un obbligo giuridico, ciò significa considerarlo anche come “soggetto in formazione”, così E. BATTELLI, *Diritto privato delle persone minori di età. Diritti, tutele, nuove vulnerabilità*, Torino, 2021, p. 4.

⁽¹³⁰⁾ COUNCIL OF EUROPE, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, cit.

⁽¹³¹⁾ Ciò al fine di fornire il più alto grado di tutela, come si evince dal report esplicativo della bozza di convenzione al §116, <https://rm.coe.int/-1497-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework-convention/1680af0734&format=native>.

⁽¹³²⁾ La differenza tra i due approcci normativi — quello del CoE e quello dell'UE — sta nella distribuzione di ruoli e responsabilità, anche in ragione delle competenze diversificate delle due istituzioni: da un lato, il Comitato dei Ministri in seno al Consiglio d'Europa si rivolge agli Stati membri della Convenzione e, pertanto, orienta le disposizioni rispetto all'individuazione di misure e interventi per regolamen-

L'approccio della Commissione UE e quello del Consiglio d'Europa appaiono accomunati dalla consapevolezza che, mentre per le altre categorie di soggetti vulnerabili, come i pazienti, la normativa di settore prevede un sistema di controllo, monitoraggio e attuazione per la commercializzazione di prodotti o erogazione di servizi dedicati, al fine di assicurare la sicurezza e l'efficacia delle relative prestazioni (si pensi all'*iter* per lo sviluppo di dispositivi medici) ⁽¹³³⁾, non sussiste, invero, un meccanismo altrettanto pervasivo per accertare la compatibilità alle specifiche esigenze di tutela per lo sviluppo e per la commercializzazione di soluzioni, applicazioni e servizi dedicati o utilizzati in larga parte dai minori di età. Conseguentemente, anche il monitoraggio dell'efficacia delle misure di mitigazione dei rischi è demandato alla percezione di sviluppatori, fornitori (*provider* e *deployer*), come parrebbe confermato dalla formulazione dell'art. 9 del Regolamento sull'IA, laddove al comma 8 si stabilisce che i prestatori di servizio siano chiamati a procedere ad una sorta di controllo del processo di valutazione di impatto, in considerazione delle diverse risultanze che potrebbero emergere per i minori di età, sempre, naturalmente, purché rispetto agli usi tale momento sia quello più appropriato ad affrontare tale verifica. Il successivo comma 9 dello stesso articolo 9, peraltro, ribadisce la necessità di effettuare la predetta valutazione aggiuntiva anche laddove si sia in presenza di sistemi considerati ad alto rischio per i quali specifiche norme di settore possono trovare applicazione.

In altri termini, la categoria dei minori di età come utenza di soluzioni basate sull'IA pretende un'attenzione particolare da parte degli operatori economici nella progettazione e sviluppo in quanto composta da soggetti vulnerabili, ma il paradigma di tutela non include meccanismi di *public enforcement*, per monitorare e certificare il buon funzionamento di tale porzione di mercato, che invece sono presenti per prodotti indirizzati ad altre categorie di soggetti vulnerabili (come

tare con normativa nazionale i sistemi di AI, tenendo conto dei principi enunciati. Diversamente, il Regolamento UE si rivolge direttamente agli operatori e, in questo senso, lo fa in maniera omnicomprensiva: distributori, fornitori, produttori, commercianti di sistemi basati sull'IA individuando specifici obblighi in ragione della tipologia della tecnologia oggetto del processo, del settore di applicazione e della categoria di soggetti cui il sistema è rivolto.

⁽¹³³⁾ Regolamento UE, 5 aprile 2017, n. 745 relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (di seguito anche "MDR").

ad esempio per i dispositivi medici rispetto ai pazienti) ⁽¹³⁴⁾. Se, da un lato, dunque, il legislatore europeo impone di disegnare, sviluppare e immettere sul mercato soluzioni che siano alla portata dei bambini, dall'altro lato, la richiesta non è supportata da meccanismi di certificazione che possano stabilire requisiti minimi di idoneità di un prodotto o di un servizio a soddisfare i diritti fondamentali dei minori di età. La valutazione FRIA (e la conseguente pubblicazione dei risultati), di cui all'art. 27 del Regolamento sull'IA, è richiesta ai *deployer* per analizzare le implicazioni sui diritti fondamentali della persona legati all'introduzione di quei sistemi ad alto rischio di cui all'allegato II dello stesso, che non a caso include quelli da implementare nel settore educativo, atti a guidare il processo di apprendimento e la relativa valutazione per ogni stato e grado di istruzione. Vedremo anche nei prossimi paragrafi come l'esigenza di tutela nella società dell'informazione sia sì comune alle legislazioni nazionali, ma lasciata alla percezione del singolo caso, senza promuovere una politica di diritto capace di identificare requisiti minimi da imporre agli operatori per l'accesso al mercato.

Sia la posizione del CoE, che quella dell'UE, inoltre, sono portatrici di un limite comune: quello di identificare le vulnerabilità come scatole dai confini ben delineati (minori, pazienti, etnia, credo religioso, etc.), legate ad elementi certi e formalmente identificabili, generalmente associati alla definizione dei dati sensibili ai sensi dell'art. 9 GDPR, lasciando all'operatore — in sede di valutazione di impatto — l'onere di rappresentare i rischi e le relative misure di mitigazione per situazioni di vulnerabilità plurime. Tale approccio non tiene conto di possibili scenari di vulnerabilità che sono propri della dimensione digitale ed espongono utenti apparentemente non portatori di alcuna vulnerabilità. In secondo luogo, la pre-determinazione delle categorie di vulnerabilità sembra essere rigida: passare da una categoria all'altra o rendere reversibile un inquadramento necessita di azioni e procedure non sempre di immediata attuazione, spesso lasciate alla ferma determinazione dell'utente di richiedere di essere espressamente dimenticato per una determinata caratteristica oppure *in toto*, con procedure che, ancora una volta, passano dall'esercizio di diritti sanciti in materia di

⁽¹³⁴⁾ E. SCALCON, *Cybersicurezza e dispositivi medici: la tutela della salute e della sicurezza dei pazienti dalle vulnerabilità informatiche nel Regolamento (UE) 2017/745 e nell'Artificial Intelligence Act*, in *BioLaw*; (1), p. 183 ss.

protezione dei dati personali ⁽¹³⁵⁾. Infatti, nell'analisi del sistema sotto il più generale profilo del divieto di discriminazioni, sono senz'altro ricomprese le valutazioni in ordine alle criticità derivanti dalla raccolta o dall'elaborazione di informazioni, che possano esporre la persona a pericoli per la propria incolumità, sicurezza e salute, ovvero fornire inferenze che incidano — includendo o escludendo o classificando — in maniera ingiustificata su parte della popolazione. Il meccanismo appare, inoltre, efficiente per i rischi noti, meno per i *bias* non noti che richiedono, come vedremo, una efficace interazione tra la fase di valutazione e quella di monitoraggio delle valutazioni di impatto ⁽¹³⁶⁾.

8. La regolamentazione della società dei dati nei sistemi extra-UE.

L'obiettivo dell'UE nella regolamentazione della società dei dati è

⁽¹³⁵⁾ Si pensi a tal proposito al diritto all'oblio e alle iniziative specifiche intraprese per evitare discriminazioni fondate sulla classificazione dell'individuo in una categoria di soggetti vulnerabili. Dal diritto all'oblio del noto caso deciso dalla Corte di Giustizia UE, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) alla l. 7 dicembre 2023, n. 193, *Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone che sono state affette da malattie oncologiche* si percepisce una evoluzione del concetto di riservatezza e di non discriminazione che pone la necessità proteggere la prerogativa dell'individuo di mantenere il controllo sulla condivisione a diversi fini delle informazioni personali, specialmente quelle di natura sensibile, sul punto si veda il rapporto dal primo anno di attuazione della legge sull'oblio oncologico AA.Vv., *Osservatorio sulla condizione assistenziale dei malati oncologici*, in *16° Rapporto sulla condizione assistenziale dei malati oncologici*, a cura di F.A.V.O., Roma 2024, e in particolare il contributo di E. IANNELLI, F. DE LORENZO, S. CINIERI, G. BERETTA, F. PERRONE, *Il diritto all'oblio oncologico: dalla legge ai decreti attuativi*, cap. 16.

⁽¹³⁶⁾ Non è questa la sede per trattare le questioni tecnico-giuridiche derivanti dai *bias* algoritmici, per cui diversi livelli di trasparenza possono essere raggiunti dai sistemi in ragione della spiegabilità dei meccanismi decisionali. Giova ricordare il caso degli sviluppatori della multinazionale Amazon che nelle procedure di *screening* delle candidature per posizioni lavorative hanno notato che — senza voler creare quell'effetto — l'algoritmo di fatto selezionasse in gran parte candidati di sesso maschile, di una certa fascia di età, con un determinato *background*. Dal monitoraggio del sistema, infatti, è emerso che la neutralità dell'algoritmo rispetto a certi *input* di fatto produceva un effetto distorsivo volto a privilegiare elementi che nella realtà caratterizzano maggiormente certe persone piuttosto che altre, si veda per una revisione aggiornata della letteratura in materia: E. ALBAROUDI, T. MANSOURI, A. ALAMEER, *A Comprehensive Review of AI Techniques for Addressing Algorithmic Bias in Job Hiring*, AI 2024, 5, 383-404. <https://doi.org/10.3390/ai5010019>.

quello di fornire un sistema coerente nei diversi settori, capace sia di rendere quanto più competitiva possibile l'economia c.d. *data-driven* europea al cospetto degli Stati Uniti e dei paesi asiatici più tecnologicamente avanzati, sia — allo stesso tempo — di garantire l'attuazione dei valori e dei diritti fondamentali della persona anche nella transizione digitale dei servizi e dei prodotti, ciò al fine di proteggerli a fronte dell'uso improprio della tecnologia.

L'influenza del GDPR sulle realtà extra-europee — prevalentemente dovuta ai meccanismi di protezione per i flussi transfrontalieri, che sono subordinati ad una decisione di adeguatezza della normativa extra EU, ovvero ad una serie di clausole contrattuali prestabilite da implementare necessariamente negli accordi fra imprese EU ed extra-EU ⁽¹³⁷⁾ — ha portato non solo a far circolare il modello basato sulla valutazione del rischio, ma addirittura ad avviare una virtuosa *cross fertilisation* ⁽¹³⁸⁾ tra buone prassi volte a introdurre nei processi di trattamento misure tecniche e organizzative *ad hoc* per la tutela dei soggetti interessati più deboli, come i bambini, in alcuni casi che illustreremo nei paragrafi che seguono.

Per questa ragione appare particolarmente interessante investigare come siano regolamentate la società dell'informazione e l'innovazione tecnologica nei sistemi appartenenti al Common Law o misti, nei sistemi asiatici tecnologicamente avanzati e, di contro, nei sistemi sudamericani o africani caratterizzati da minori investimenti nelle infrastrutture digitali e tecnologiche, al fine di trarne indicazioni operative con riferimento alla comune percezione delle vulnerabilità nella dimensione digitale e alle possibili buone prassi adottate per risolvere questioni applicative controverse comuni.

Dalla mappatura, come vedremo, emerge che le problematiche relative alla protezione e promozione dei minori di età nell'ambiente digitale sono da considerarsi comuni a prescindere dalle caratteristiche del sistema giuridico, o dalla scelta del legislatore di disciplinare un settore specifico, piuttosto che un altro. Osserveremo, inoltre, che l'attenzione verso gli utenti minori di età nelle iniziative legate alla digitalizzazione dei sistemi non dipende dall'avanzamento dei processi di transizione digitale dei servizi e dei prodotti. Ad esempio, sul piano

⁽¹³⁷⁾ Capo V, GDPR.

⁽¹³⁸⁾ C. GIORGETTI M. POLLACK, *Beyond Fragmentation Cross-Fertilization, Cooperation and Competition among International Courts and Tribunals*, Cambridge Un. Press, 2022.

dell'autoregolamentazione internazionale, i Principi di Hiroshima, che costituiscono un primo codice di condotta per sviluppatori di sistemi avanzati di IA di tutto il mondo, si riferiscono ai minori solo una volta nell'ambito dell'identificazione delle aree di ricerca volte a mitigare i rischi dell'IA per la società ⁽¹³⁹⁾.

Per tali ragioni, diventa interessante identificare nelle risposte fornite dai vari sistemi giuridici analizzati quei fattori comuni o particolarmente efficaci, capaci di poter contribuire a disegnare un paradigma di protezione, promozione e attuazione dei diritti dei minori di età nella dimensione digitale e rispetto alle nuove tecnologie che possa circolare — con opportuni adattamenti — nelle diverse famiglie giuridiche, offrendo strategie regolatorie sufficientemente armonizzate da poter far dialogare gli istituti di diritto privato di volta in volta coinvolti con gli *standard* tecnici elaborati e riconosciuti ⁽¹⁴⁰⁾.

8.1. *I sistemi di Common Law.*

Il sistema di *common law* maggiormente influenzato dall'approccio dell'UE è senz'altro quello britannico che, addirittura, prima della *brexit*, svolgeva tra gli Stati Membri un ruolo di armonizzatore delle prassi per l'attitudine dell'Information Commissioner's Office (di seguito anche "ICO") a disegnare scenari applicativi e sviluppare linee guida per gli operatori, mutuabili in tutta Europa. Conseguentemente, la legislazione nazionale sulla *privacy* — il Data Protection Act del 2018

⁽¹³⁹⁾ Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems, 30 ottobre 2023, <https://www.mofa.go.jp/files/100573473.pdf>.

⁽¹⁴⁰⁾ Diversi studi interdisciplinari si apprestano a testare l'efficacia della normativa a tutela dei minori: N. VLAJIC, M. EL MASRI, G. M. RIVA, M. BARRY, AND D. DORAN (2018), *Online Tracking of Kids and Teens by Means of Invisible Images: COPPA vs. GDPR*. In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS '18). Association for Computing Machinery, New York, NY, USA, 96-103. <https://doi.org/10.1145/3267357.3267370>; O. FIGUEIRA, R. TRIMANANDA, A. MARKOPOULOU, S. JORDAN (2024) *DiffAudit: Auditing Privacy Practices of Online Services for Children and Adolescents*, in Proceedings of the 2024 ACM on Internet Measurement Conference (IMC '24). Association for Computing Machinery, New York, NY, USA, 488-504. <https://doi.org/10.1145/3646547.3688416>; M. MACENAITE, E. KOSTA, *Consent for processing children's personal data in the EU: Following in US Footsteps?*, 26(2) Information & Communications Technology Law, at p. 181.

— ha, naturalmente, ricevuto la decisione di adeguatezza, all'indomani dell'uscita del Regno Unito dall'UE ⁽¹⁴¹⁾.

Rispetto all'IA, la strategia governativa non prevede attualmente l'elaborazione di una normativa *ad hoc*, ma ha dato mandato alle autorità indipendenti ⁽¹⁴²⁾ di promuovere valutazioni di impatto inter-settoriali in modo da non vincolare diritti e obblighi a uno scenario in evoluzione, come quello del progresso tecnologico basato sull'IA. Per quanto concerne, invece, le piattaforme digitali, nell'aprile 2023 è stata avanzata una proposta, il c.d. Digital Markets, Competition and Consumers Bill ⁽¹⁴³⁾, volto a regolamentare la concorrenza nella dimensione digitale e a tutelare i consumatori-utenti sulla scia del Digital Markets Act europeo.

L'iniziativa più interessante ai nostri fini è quella relativa all'Online Safety Act, promulgato nel settembre 2023, che si propone di rendere *internet* un ambiente più sicuro per le persone nel Regno Unito ⁽¹⁴⁴⁾. A tal fine sono imposti obblighi ai fornitori di servizi digitali affinché identifichino, mitighino e gestiscano i rischi derivanti dalla pubblicazione di contenuti e attività illegali *online*, in generale, e che rechino pregiudizio ai bambini. La normativa, come vedremo meglio nel prossimo capitolo — dove analizzeremo gli strumenti di protezione suscettibili di circolare tra gli ordinamenti in termini di buone prassi capaci di armonizzare le soluzioni — è strutturata in modo da rendere la dimensione digitale alla portata dei minori di età attraverso il noto meccanismo di introduzione di obblighi di *due diligence* e di valutazione del rischio, sviluppando in maniera più articolata i profili rilevanti per la tutela degli utenti minori di età andando a differenziare tipologie di pericoli e contromisure.

⁽¹⁴¹⁾ Commissione Europea, decisione di adeguatezza del 28 giugno 2021.

⁽¹⁴²⁾ Oltre all'ICO, la Financial Conduct Authority (FCA), la Competitions and Markets Authority (CMA) e la Medicines & Healthcare products Regulatory Agency (MHRA).

⁽¹⁴³⁾ Gli emendamenti saranno discussi nell'estate 2024, <https://bills.parliament.uk/bills/3453>. I. COFONE, *Traditionalist Data Protection Rules*, in *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge: Cambridge University Press, 2024).

⁽¹⁴⁴⁾ Online Safety Act 2023, <https://www.legislation.gov.uk/ukpga/2023/50/enacted>.

8.2. *Il Digital Charter Implementation Act canadese e il Codice civile del Québec.*

Il Canada è stato uno dei primi stati a introdurre una strategia sull'IA già nel 2017. Più recentemente, è stata pubblicata una ampia iniziativa legislativa federale, il c.d. Digital Charter Implementation Act del 2022 ⁽¹⁴⁵⁾, che mira a regolamentare sia dal punto di vista sostanziale, con il Consumer Privacy Protection Act ⁽¹⁴⁶⁾, che processuale, con il Personal Information and Data Protection Tribunal Act, la posizione dell'utente-soggetto interessato-consumatore rispetto alla gestione delle proprie informazioni personali, nonché a introdurre requisiti per garantire la sicurezza e l'equità dei sistemi ad alto impatto basati sull'IA, con l'Artificial Intelligence and Data Act (AIDA) ⁽¹⁴⁷⁾. Il Digital Charter Implementation Act consta di tre parti, che sono state pubblicate in momenti diversi. Le prime due mirano ad incrementare il controllo sulle informazioni conferite e sui livelli di trasparenza, disciplinando — ad esempio — il diritto alla portabilità, all'oblio e stabilendo un sistema di *enforcement* rispetto agli obblighi imposti e istituendo autorità con specifici poteri ispettivi e sanzionatori.

L'AIDA, invece, si propone di mantenere con riferimento ai sistemi di IA lo stesso livello di protezione dei diritti umani e della sicurezza delle persone delle altre due parti del testo unico, anche grazie all'introduzione di meccanismi di consultazione con le categorie di parti interessate. In particolare, l'AIDA disciplina obblighi di valutazione e mitigazione dei rischi sia nella fase di progettazione, che di sviluppo e implementazione dei sistemi ad alto impatto, attraverso meccanismi di monitoraggio e aggiornamento delle misure di protezione. La proposta canadese, al pari dell'approccio europeo, introduce norme quanto più possibilmente adattabili allo sviluppo delle potenzialità dell'IA, identificando limiti e divieti, prevedendo un crescendo

⁽¹⁴⁵⁾ C-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (Digital Charter Implementation Act), 16 giugno 2022, <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>.

⁽¹⁴⁶⁾ Queste iniziative legislative mirano ad incrementare il controllo sulle informazioni conferite e sui livelli di trasparenza, disciplinando il diritto alla portabilità, all'oblio e stabilendo un sistema di *enforcement* rispetto agli obblighi stabiliti.

⁽¹⁴⁷⁾ N. TAFAZOLI, *Crossing the Digital Rubicon: Recalibrating Private Power for Public Purpose by Centering Rights, Risks, and Harms in the Artificial Intelligence and Data Act*, 82 U. Toronto Fac. L. Rev. 51.

di obblighi in ragione della gravità o probabilità di occorrenza dei rischi collegati ad una determinata funzione o processo automatizzato cui sono associati meccanismi di monitoraggio e controllo demandati alla costituzione di uffici *ad hoc*. Al Ministro dell'Innovazione, della Scienza e dell'Industria è conferito, inoltre, il potere di amministrare e far rispettare le disposizioni dell'AIDA al fine di consentire una armoniosa evoluzione del sistema politico economico con lo sviluppo tecnologico, anche attraverso il supporto di un ufficio competente, l'AI and Data Commissioner, con compiti di formazione e assistenza alle attività di *compliance*.

Con riferimento ai minori di età, il Consumer Privacy Protection Act abbraccia un approccio in larga parte condiviso, come vedremo, anche in altri ordinamenti, ossia quello relativo alla qualificazione delle informazioni concernenti il soggetto minorenni nell'alveo dei dati sensibili, consentendo così l'automatica applicazione del regime previsto per le informazioni che rivelano una vulnerabilità del soggetto interessato ⁽¹⁴⁸⁾. Questa modalità ha il pregio di proteggere gli utenti minorenni rispetto alla confidenzialità, integrità e disponibilità dei flussi informativi che li riguardano, ma la stessa potrebbe non risultare sufficiente per prevenire i rischi specifici che espongono, in particolare, l'utente con limitata capacità di discernimento, laddove la misura non sia accompagnata da ulteriori misure di salvaguardia. A questo proposito, lo stesso Consumer Privacy Protection Act replica per i minori di età le considerazioni in ordine al principio di minimizzazione, limitando anche il diritto delle organizzazioni a raccogliere o conservare per ulteriori usi informazioni sui minori, ammonendo in ogni caso gli operatori di assicurare elevati *standard* di protezione: pertanto il principio di limitazione della finalità è interpretato restrittivamente allorché si tratti di consumatori minorenni, anche nelle ipotesi in cui l'informazione personale sia raccolta necessariamente per assicurare l'accurata erogazione di un servizio o prodotto, o in caso di conservazione orientata alla successiva restituzione di flussi di dati raccolti al medesimo interessato ⁽¹⁴⁹⁾. Relativamente all'esercizio dei diritti, inol-

⁽¹⁴⁸⁾ (2) "*Interpretation — minors. For the purposes of this Act, the personal information of minors is considered to be sensitive information*".

⁽¹⁴⁹⁾ La norma si ricava da una lettura *a contrario* dell'art 55, *Exception (2)* "An organization may refuse a request to dispose of personal information in the circumstances described in paragraph (1)(b) or (c) if (...) (d) the information is not in relation to a minor and the disposal of the information would have an undue adverse impact on the accuracy

tre, la rappresentanza legale espressa dal genitore è temperata dall'eventuale volontà dell'interessato di “*personally exercise those rights and recourses and is capable of doing so*”: per cui il diritto di disporre dei propri dati da parte del minore non può essere limitato al minore che dimostri capacità di discernimento ⁽¹⁵⁰⁾. A questo proposito la normativa risulta lacunosa in termini di sensibilizzazione ed educazione digitale, soprattutto rispetto ai menzionati meccanismi di valorizzazione dell'autonomia e del controllo del minore di età.

L'esperienza del Québec merita attenzione rispetto alle altre province in quanto ha elaborato una normativa volta ad adeguare le esistenti tutele in materia di protezione dei dati personali alle sfide tecnologiche, introducendo, in particolare sanzioni private in materia di trattamento illecito di dati personali ⁽¹⁵¹⁾. In particolare, la *Loi sur la protection des renseignements personnels dans le secteur privé*, merita menzione in questo contesto sebbene si ponga (per struttura e tecnica legislativa) in armonia con le iniziative normative tipiche dei sistemi di *civil law*, in quanto introduce ciononostante una fattispecie autonoma di danno punitivo, tradizionalmente legata alle esperienze di *common law*. Infatti, ai sensi del riformato articolo 93, in caso di violazione intenzionale, o per colpa grave, di un diritto conferito dalla stessa *Loi*, o dagli articoli da 35 a 40 del codice civile del Québec, che abbia provocato un pregiudizio, è attribuito al tribunale il potere di liquidare d'ufficio una somma di ammontare pari ad almeno mille dollari canadesi. L'esempio si pone a corroborazione dell'intento del legislatore di costruire un paradigma efficace anche in termini di attuazione, sfruttando le potenzialità di deterrenza non solo del Commissioner, come

or integrity of information that is necessary to the ongoing provision of a product or service to the individual in question; (...) (f) the information is not in relation to a minor and it is scheduled to be disposed of in accordance with the organization's information retention policy, and the organization informs the individual of the remaining period of time for which the information will be retained”.

⁽¹⁵⁰⁾ Sul punto, l'UNICEF Canada ha commentato la proposta suggerendo di introdurre un correttivo orientato a raccogliere l'opinione del minore sull'esercizio dei propri diritti a mezzo del rappresentante legale, ovvero a specificare che l'intervento del rappresentante debba seguire il principio di interesse superiore del fanciullo, UNICEF CANADA, Bill C-27 Digital Charter Implementation Act, 2022, <https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12448397/br-external/UNICEFCan-e.pdf>.

⁽¹⁵¹⁾ Bill 64, ora Law 25, *Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c. 25.

private enforcement, ma autorizzando eccezioni al principio di risarcimento integrale da parte dell'autorità giudiziaria ⁽¹⁵²⁾. In questo senso, si apprezza il tentativo di trovare una misura complementare alla prevenzione dei rischi per i soggetti minori di età che possa promuovere una robusta attuazione della tutela.

8.3. *L'approccio negli USA e le iniziative statali: cenni.*

Non diversa appare la posizione presa in una seduta pubblica del Senato degli Stati Uniti d'America del settembre 2023, dove è stata discussa la possibilità di regolamentare al livello federale l'IA, specificando la necessità di istituire una agenzia *ad hoc* per il monitoraggio e controllo dei sistemi. Diverse sono le proposte normative avanzate: vi è il SAFE Innovation AI Framework, che si propone di stabilire dei principi comuni per sviluppatori, aziende e *policy maker* ⁽¹⁵³⁾, nonché ulteriori iniziative, per lo più di settore, sono state pubblicate per

⁽¹⁵²⁾ Il dibattito sui danni punitivi in Québec è ampio e complesso, come in tutti i sistemi di *civil law*. L'art. 1621 del codice civile del Québec, ne consente la liquidazione, limitando tuttavia la portata al soddisfacimento della funzione preventivo-deterrente, individuando peraltro dei parametri di valutazione, come la “*gravità della colpa del debitore, della sua situazione finanziaria o dell'entità dell'indennizzo che è già tenuto a versare al creditore (...) del fatto che il pagamento della riparazione sia, in tutto o in parte, assunta da un terzo*”, M. SANSON, *Les dommages punitifs en droit Québécois: tradition, evolution... et revolution*, (2012) 42 R.D.U.S, 159 ss., J.L. BAUDOUIN, *Tort Law in Québec*, Wolters Kluwer, 2019, p. 259 ss. In Italia, il dibattito sulle funzioni della responsabilità civile ha toccato in più occasioni il tema dell'ammissibilità o meno di danni cc.dd. punitivi anche al di là dei procedimenti di delibazione e dell'interpretazione della clausola dell'ordine pubblico. Cass., sez. un., 5 luglio 2017, n. 16601, in *Foro it.*, 2017, I, p. 2613, con note di A. PALMIERI, R. PARDOLESI, P.G. MONATERI; E. D'ALESSANDRO, R. SIMONE. In dottrina, F.D. BUSNELLI, *La funzione deterrente e le nuove sfide della responsabilità civile*, in *La funzione deterrente della responsabilità civile*, a cura di P. SIRENA, Milano, 2011, 42, A. GAMBARO, *Le funzioni della responsabilità civile tra diritto giurisprudenziale e dialoghi transnazionali*, in *Nuova giur. civ.*, 2017, II, p. 1406, P.G. MONATERI, *Le Sezioni Unite e le molteplici funzioni della responsabilità civile*, in *Nuova giur. civ.*, 2017, II, p. 1410, G. PONZANELLI, *I danni punitivi oltre la delibazione delle sentenze straniere?*, in *Jus civile*, 2018, p. 42 ss.

⁽¹⁵³⁾ I principi informativi della materia sono stati individuati nei già noti concetti al livello europeo di *security*, *accountability* ed *explain(ability)* e nelle più propriamente statunitensi espressioni di *foundation*, per richiamare i valori costituenti, e *innovation* per sottolineare il ruolo USA nello sviluppo tecnologico, così SAFE Innovation Framework, 2023, https://www.democrats.senate.gov/imo/media/doc/schumer_ai_framework.pdf. Per un approfondimento, M. E. KAMINSKI, *Regulating the Risks of AI* (2023) 103 BUL Rev 1348 at 1374.

facilitare la valutazione dell'impatto e dell'uso dell'IA, anche di tipo generativo, in scenari particolarmente critici, come nelle campagne elettorali ⁽¹⁵⁴⁾, o nelle attività di sorveglianza nei luoghi di lavoro ⁽¹⁵⁵⁾, o finalizzate alla lotta alla disinformazione ⁽¹⁵⁶⁾, o nelle altre attività di ricerca e sviluppo ⁽¹⁵⁷⁾.

Al livello di legislazione statale vi sono numerose proposte formulate per la regolamentazione dell'IA, ma solo il Connecticut ⁽¹⁵⁸⁾ e il Texas ⁽¹⁵⁹⁾ hanno completato l'*iter* di adozione di normative istitutive di commissioni di valutazione di sistemi di IA sviluppate dalle pubbliche amministrazioni, affinché non producano effetti discriminatori nei processi decisionali dei servizi pubblici. Diverse questioni legate agli effetti distorsivi delle nuove tecnologie sono, invece, oggetto di intervento giurisprudenziale ⁽¹⁶⁰⁾.

Il quadro si presenta notevolmente frammentario e settoriale e appare difficile individuare elementi utili alla costruzione di un paradigma volto a qualificare la transizione digitale dei diritti dei minori.

⁽¹⁵⁴⁾ REAL Political Advertisement Bill, <https://www.congress.gov/bill/118th-congress/senate-bill/1596/text>. Per una disamina più completa dei rischi per la democrazia, cfr. K. MANHEIM; L. KAPLAN, *Artificial Intelligence: Risks to Privacy and Democracy*, Yale Journal of Law and Technology 21 (2019): 106-188.

⁽¹⁵⁵⁾ Stop Spying Bosses Act, <https://www.congress.gov/bill/118th-congress/senate-bill/262/text>.

⁽¹⁵⁶⁾ https://www.coons.senate.gov/imo/media/doc/no_fakes_act_one_pager.pdf.

⁽¹⁵⁷⁾ Artificial Intelligence Research, Innovation, and Accountability Act of 2023, che incorpora altresì le raccomandazioni del National Institute of Standards and Technology Act (NIST) <https://www.congress.gov/bill/118th-congress/senate-bill/3312/text>.

⁽¹⁵⁸⁾ <https://www.cga.ct.gov/2023/act/Pa/pdf/2023PA-00016-R00SB-01103-PA.PDF>.

⁽¹⁵⁹⁾ <https://capitol.texas.gov/tlodocs/88R/billtext/html/HB02060F.htm>. Sul punto Z. TAKHSHID, *Children's Digital Privacy and the Case Against Parental Consent*, Texas L. R., 2023, 101, 3.

⁽¹⁶⁰⁾ Ad es., la US District Court della Columbia ha affermato l'estate scorsa che non vi possa essere tutela di diritti di proprietà intellettuale in casi di sviluppo di contenuti esclusivamente da parte di sistemi di intelligenza artificiale, specificando che si aprono nuovi dubbi interpretativi sulla valutazione dell'apporto creativo del singolo rispetto all'uso di sistemi IA addestrati su opere preesistenti sconosciute *Thaler v. Perlmutter*, Case No. 1:22-cv-01564, (D.D.C. 2022), the United States District Court for the District of Columbia, disponibile su https://cdn.patentlyo.com/media/2023/08/THALER-v.-PERLMUTTER-et-al-Docket-No.-1_22-cv-01564-D.D.C.-Jun-02-2022-Court-Docket-1.pdf. In dottrina: A. CHANDER, M. E. KAMINSKI, W. McGEVERAN, *Catalyzing Privacy Law*, 105 Minnesota L. Rev. 1733 (Aprile 2021).

Tra le prime disposizioni federali sulla protezione dei dati e servizi della società dell'informazione vi è il COPPA (Children's Online Privacy Protection Act) che, nel prevedere certi requisiti da applicare agli operatori di siti web o servizi online rivolti a bambini che non abbiano compiuto il tredicesimo anno di vita ⁽¹⁶¹⁾, stabilisce come base giuridica del trattamento delle informazioni personali dei minori di età la previa acquisizione di un “*verifiable parental consent*”, lasciando alla Federal Trade Commission il compito di indicare, in ragione dell'evoluzione delle tecnologie, le metodologie che garantiscono all'operatore economico di provare la conformità alle verifiche richieste e di rendere pubblici i risultati ⁽¹⁶²⁾.

Nel prossimo capitolo analizzeremo le misure tecniche e organizzative introdotte nelle prassi statunitensi a tutela dei minori nello spazio digitale anche alla luce di alcune esperienze di legislazione statale che, prevedendo specifici divieti e limiti per i giovani utenti, richiedono l'adozione di strumenti e funzioni *ad hoc*, stimolando il dibattito in ordine al bilanciamento di interessi contrapposti.

9. I sistemi tecnologicamente avanzati in Asia e Oceano Pacifico.

Le normative nazionali dell'area asiatica e dell'oceano pacifico si occupano da oltre un decennio di disciplinare la rilevanza penale di

⁽¹⁶¹⁾ Sulla base, infatti, Children's Online Privacy Protection Act del 1998 e ss.mm.ii. per bambino si intende chi non abbia compiuto gli anni tredici, diversamente dalla definizione offerta dalla CRC, <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim>. È da osservare che una proposta di modifica e aggiornamento della normativa è attualmente in discussione per consentire un'estensione della tutela prevista dal COPPA a tutti i bambini, fino al compimento del diciassettesimo anno di età: COPPA 2.0., Children and Teens' Online Privacy Protection Act, S.1418 — 118th Congress (2023-2024), <https://www.congress.gov/bill/118th-congress/senate-bill/1418/text>.

⁽¹⁶²⁾ *Infra* Cap. 2, §3.1. Sul COPPA: A. O'DONNELL (2020) *Why the vppa and coppa are outdated: how netflix, youtube, and disney+ can monitor your family at no real cost*. Georgia Law Review, 55(1), 467; M. L. HERSH, *Is Coppa a Cop Out - The Child Online Privacy Protection Act as Proof That Parents, Not Government, Should Be Protecting Children's Interests on the Internet*, 28 Fordham Urb. L.J. 1831; G. MALDOFF - O. TENE, *Born in the USA: The GDPR and the Case for Transatlantic Privacy Convergence*, 17 Colo. Tech. L.J. 295 (2019); M. W. BERG, *COPPA as Catalyst: Recalibrating the FTC's Privacy Enforcement Framework*, 75 Rutgers U.L. Rev. 1011 (2023); E. HABER (2020). *The internet of children: protecting children's privacy in hyper-connected world*. University of Illinois Law Review, 2020(4), 1209-1248.

alcuni illeciti perpetrati anche nella dimensione digitale contro i bambini: dalla pornografia minorile, all'abuso sessuale, etc. Più di recente i sistemi con più alta penetrazione digitale nei settori economici hanno cominciato a regolamentare fenomeni specifici della datificazione della società, come il *cyberbullismo* (punito in Australia, Nuova Zelanda, Filippine e Singapore) ⁽¹⁶³⁾ e a introdurre norme specifiche a tutela della *privacy* e per la lotta alla dipendenza digitale ⁽¹⁶⁴⁾.

Tra questi l'Australia, che aveva già promulgato l'*Enhancing Online Safety for Children Act* nel 2015, ne ha aggiornato la versione nel 2021, formulando un sistema di protezione rispetto dall'esposizione a materiale e contenuti che non siano idonei ad essere trattati da minori di età ⁽¹⁶⁵⁾. Si sposta in questo contesto la soglia di responsabilizzazione, elevandosi, dalla mera liceità, finalizzata a non arrecare pregiudizi (similmente al DSA), alla più generale garanzia di idoneità rispetto all'infanzia. Il parametro di riferimento non è — dunque — solo legato alla verifica della liceità o meno dei contenuti, ma anche ad un apprezzamento di appropriatezza e adeguatezza degli stessi rispetto alle caratteristiche dell'utente ⁽¹⁶⁶⁾. Ciò implica la necessità per lo sviluppatore di introdurre competenze specifiche di tipo umanistico e sociale che siano di supporto nel ciclo di vita della progettazione del sistema per orientare tale apprezzamento. La normativa, inoltre, abbraccia il *favor* per l'autoregolamentazione — comune alla strategia europea — degli operatori economici promuovendo, nell'elenco dei possibili contenuti dei codici di condotta industriali, l'opzione di indicare ai genitori come supervisionare e controllare l'accesso dei minori ai *social media* e agli altri servizi elettronici e digitali, nonché come impedire l'apertura

⁽¹⁶³⁾ J. LEE, Y. PING HSIEH, R. THORNBURG, *An Introduction to the Special Issue on Cyberbullying in Asia and Pacific: Its Nature and Impact*, Asia Pacific Journal of social work and development 30.3 (2020), 145; A. SRIVASTAVA, J. BOEY, *Online Bullying and Harassment: An Australian Perspective*, 6 Masaryk U. J.L. & Tech. 299 (2012).

⁽¹⁶⁴⁾ Sul punto, uno studio finanziato da Google, elaborato da Internet Society, *Mapping Online Child Safety in Asia-Pacific*, 2017, disponibile <https://www.icmec.org/wp-content/uploads/2018/08/Mapping-Online-Safety-in-11-Asian-Countries-Internet-Society.pdf>.

⁽¹⁶⁵⁾ Il paragrafo 108 attribuisce al Commissioner il potere di limitare l'accesso ai contenuti online laddove “*the objective of protecting children from exposure to material that is unsuitable for children*”. Per una ricostruzione, si veda: M. MARCOWITZ-BITTON, H. SOMMER (2022). *Remedying online shaming*. Cardozo International & Comparative Law Review, 5(2), 375-414.

⁽¹⁶⁶⁾ Vedremo che questo approccio non è isolato, *infra* § 9.3.

di profili senza il consenso dei genitori. Ancora più di recente, il Parlamento ha approvato l'Online Safety Amendment (Social Media Minimum Age) Bill 2024, che vieterà a partire da gennaio 2026 l'uso di *social media* a minori di anni sedici, prevedendo per i fornitori di piattaforme che consentono secondo i loro termini e condizioni l'accesso a utenti di età inferiore, di “*adottare misure ragionevoli per impedire*” agli utenti sotto soglia di avere un *account*, stabilendo anche delle sanzioni consistenti in caso di violazione ⁽¹⁶⁷⁾.

A questo proposito, nell'ottica di individuare elementi rilevanti ai fini della circolazione dei modelli possiamo cogliere — da un lato — il crescente ruolo attribuito dai legislatori ai codici di condotta come strumento di definizione, implementazione e monitoraggio di pratiche virtuose — dall'altro — la riflessione in ordine all'opportunità di predisporre dei regimi differenziati tra bambini e adolescenti, dall'altro ancora, la necessità di accompagnare le iniziative con interventi volti a un cambiamento culturale rivolto direttamente ai minori di età per poterli preparare ad un uso quotidiano e consapevole delle nuove tecnologie.

9.1. *La tutela dei dati personali “adeguata” in Corea del Sud e Giappone e i relativi approcci verso i minori di età.*

Nel contesto di economie fortemente caratterizzate dal fenomeno della datificazione, merita un approfondimento la legislazione a tutela della protezione dei dati adottata nella Corea del Sud, che risale al 2011 ⁽¹⁶⁸⁾, modificata sia nel 2021, che, più di recente, nel 2023 ⁽¹⁶⁹⁾. La stessa ha ricevuto la decisione di adeguatezza da parte della Com-

⁽¹⁶⁷⁾ L'obiettivo della modifica è quello di minimizzare il rischio di esposizione, alla stregua dei divieti di somministrare alcool o sigarette agli adolescenti. Peraltro si esclude che la restrizione possa riguardare applicazioni di messaggistica, giochi online e servizi che abbiano come primo scopo il supporto al diritto alla salute o all'educazione dell'utente, così *Explanatory Memorandum*, Online Safety Amendment (Social Media Minimum Age) Bill 2024, https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r7284_ems_b9c134ac-a19a-47b2-9879-b03dda6e3c1a/upload_pdf/JC014726.pdf;fileType=application%2Fpdf.

⁽¹⁶⁸⁾ G. GREENLEAF - P. WHON-IL, *South Korea's Innovations in Data Privacy Principles: Asian Comparisons*, *The computer law and security report* 30.5 (2014): 492-505.

⁽¹⁶⁹⁾ South Korea, the Personal Information Protection Act (PIPA), Act No. 10465, Mar. 29, 2011 e ss.mm.ii, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG. K. DONG HYEON - D. HYUN PARK, *Automated Decision-Making in*

missione Europea ai sensi dell'art. 45 GDPR e difatti si riscontrano numerosi punti di contatto con il sistema di tutele dell'UE: dall'enunciazione dei principi di minimizzazione e finalità, al riconoscimento del diritto alla portabilità, al divieto di profilazione, all'individuazione di figure di consulenza obbligatoria per le pubbliche amministrazioni, come il responsabile per la protezione dei dati, prevedendo livelli di conformità diversificati a seconda che si tratti di titolari del trattamento di tipo ordinario, ovvero prestatori di servizi *online*.

La tutela dei minori di età si articola in alcuni divieti, obblighi e sanzioni. In particolare, l'articolo 22 della legge, dedicato ai metodi per ottenere il consenso dell'interessato, specifica che, in caso di utente che non abbia compiuto gli anni quattordici, occorre raccogliere il consenso del legale rappresentante, il quale avrà anche il potere di esercitare i diritti per conto del bambino ⁽¹⁷⁰⁾. A differenza di altre iniziative legislative, come il DSA, che in applicazione del principio di minimizzazione vieta espressamente la raccolta di dati ulteriori, nel sistema in esame, si precisa che informazioni personali minimali che siano necessarie ad ottenere il consenso del legale rappresentante possono essere raccolte direttamente dall'infraquattordicenne, senza il consenso dell'adulto ⁽¹⁷¹⁾. In caso di prestatori di servizi di informazione e comunicazione, peraltro, il consenso espresso dal legale rappresentante deve essere oggetto di conferma (art. 39-3, comma 4) e la notifica del fatto che vi siano attività di trattamento di dati personali di minori di anni quattordici deve essere resa all'interessato stesso con linguaggio semplice e immediatamente comprensibile. L'autorità garante deve poi porre in essere delle misure di salvaguardia particolari volte a tutelare l'infraquattordicenne che potrebbe non comprendere i rischi e gli effetti legati al trattamento di informazioni personali e non essere a conoscenza dei propri diritti ⁽¹⁷²⁾. La disposizione, quindi, facilita

South Korea: A Critical Review of the Revised Personal Information Protection Act, in *Humanities & social sciences communications* 11.1 (2024): 974-11.

⁽¹⁷⁰⁾ L'art. 38, comma 2 sull'accesso, prevede che sia il legale rappresentante ad esercitare i diritti per il minore di anni quattordici.

⁽¹⁷¹⁾ Così l'art. 22 "*When it is required to obtain consent pursuant to this Act to process personal information of a child under 14 years of age, a personal information controller shall obtain the consent of his or her legal representative. In such cases, minimum personal information necessary to obtain the consent of the legal representative may be collected directly from such child without the consent of his or her legal representative*".

⁽¹⁷²⁾ Così l'art. 39-3, comma 6.

l'acquisizione di informazioni dall'utente per consentire l'applicazione del regime a seconda dell'età. Come misure organizzative di salvaguardia dei flussi di dati raccolti, poi, si esplicitano quelle derivanti dal principio di trasparenza, quando probabilmente un richiamo a quello di minimizzazione avrebbe potuto formulare indicazioni sul periodo di conservazione ed eventuale distruzione delle stesse una volta raggiunta la finalità di inquadrare l'utente nella fascia di età rappresentata. Da rimarcare, altresì, il ruolo dell'autorità di controllo nelle attività di promozione di campagne di sensibilizzazione ai rischi e presa di coscienza dei diritti per l'utente bambino.

Anche la normativa giapponese sulla protezione dei dati personali, risalente al 2003 e recentemente modificata ⁽¹⁷³⁾, ha ricevuto la decisione di adeguatezza dalla Commissione Europea, tuttavia, la stessa non prevede alcuna disposizione *ad hoc* a tutela dei minori di età. Inoltre, il Giappone non si è ancora dotato di una regolamentazione sull'IA, infatti, alcune linee guida sono state adottate nel 2022 dal Ministero dell'Economia, Commercio e Industria ⁽¹⁷⁴⁾, ma non costituiscono norma cogente e non menzionano in alcuna parte i minori di età ⁽¹⁷⁵⁾. Le stesse, infatti, non si discostano eccessivamente dai sette requisiti della c.d. ALTAI *checklist*: menzionano esplicitamente la *literacy* come valore fondante, che emerge anche dal testo dell'AI Act europeo, e l'*innovation* che, invece, riguarda la collaborazione tra portatori di interesse per il progresso scientifico e tecnologico, anch'esso riconducibile al *favor* europeo verso meccanismi virtuosi di coinvolgimento sin dalla progettazione degli attori portatori di interessi. Nemmeno la

⁽¹⁷³⁾ Act on the Protection of Personal Information (Act No. 57 of 2003), <https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>. J. MOON-HO - H. YEONG KWON, *Comparison of Personal Information De-Identification Policies and Laws within the EU, the US, Japan, and South Korea*, in *Government information quarterly* 40.2 (2023): 101805.

⁽¹⁷⁴⁾ Linee Guida METI incorporate nel AI Governance in Japan Report, https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_8.pdf. Nelle more della pubblicazione del presente volume, il sistema giapponese si è dotato di uno strumento legislativo in materia di cooperazione multilivello nella ricerca, sviluppo e utilizzo dell'IA: Bill on Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies, 28.2.2025.

⁽¹⁷⁵⁾ Anzi, la circostanza di perseguire il benessere del minore può costituire una eccezione alle procedure identificate per i titolari del trattamento, così artt. 18, 20, 27.

regolamentazione sulle piattaforme digitali approvata nel 2020 ⁽¹⁷⁶⁾, che si propone di migliorare la trasparenza e l'equità di determinate piattaforme digitali, affronta il tema della protezione dell'utente minore di età.

Le similitudini con il sistema di tutele dell'UE potrebbero pertanto consentire di influenzare i processi legislativi, facilitando l'implementazione di quelle buone prassi che andremo a selezionare nel prossimo capitolo.

9.2. *Il sistema cinese: cenni e rinvio.*

Diversamente rispetto a quanto osservato per il Giappone, il sistema cinese, così come riformato nel 2023 ⁽¹⁷⁷⁾, presta particolare attenzione alla tutela dei minori, definendo requisiti e condizioni per il trattamento di informazioni personali degli infraquattordicenni, notevolmente stringenti rispetto al regime generale, e provvedendo ad indicare specifiche iniziative per procedere ad una efficace valutazione di impatto che tenga conto delle esigenze dei minori in ragione della fascia di età di appartenenza. In particolare, come vedremo in dettaglio nel prossimo capitolo, l'articolo 28 del Personal Information Protection Law ⁽¹⁷⁸⁾ definisce i dati dei minori di quattordici anni come “*dati personali sensibili*”. L'articolo 31 della stessa iniziativa legislativa impone di ottenere il consenso dei genitori o dei tutori del minore per il trattamento dei dati personali del bambino, stabilendo specifiche condizioni per l'accertamento dell'età in caso di utente di servizi della società dell'informazione. La previsione impone, tuttavia, un bilanciamento di interessi rispetto all'art 145 del codice civile cinese, letto in combinato disposto con l'art. 19, che considera i bambini che abbiano

⁽¹⁷⁶⁾ Act No. 38 of 2020, *Act on Improving Transparency and Fairness of Digital Platforms*, per un commento F. DAVIES, *Japan*, in *Digital Markets Regulation Handbook*, 2024, Cleary Gottlieb.

⁽¹⁷⁷⁾ Regolamento sulla protezione dei minori in Internet, 24 ottobre 2023, in vigore dal giorno 1 gennaio 2024, disponibile https://www.cac.gov.cn/2023-10/24/c_1699806932316206.htm.

⁽¹⁷⁸⁾ Provisions on Online Protection of Children's Personal Information, 22.08.2019, <https://perma.cc/2RJZ-XN98> per un commento J. GONG, *China Strengthens the Protection of Minors in Cyberspace*, Bird & Bird, 2023; R. YANG GAO, *Personal Information Protection under Chinese Civil Code: A Newly Established Private Right in the Digital Era*, 13 Tsinghua China L. Rev. 165 (Fall 2020); B. VERRI ET AL., *The Chinese Frontiers Of Data Protection: The Personal Information Protection Law (PIPL)*, in Philosophical Studies Series. Vol. 154. Switzerland: Springer, 2023. 181-197.

compiuto otto anni quali soggetti a incapacità limitata, consentendo — tenuto conto di alcuni fattori, tra cui l'età, lo stato di salute anche mentale e la capacità cognitiva — di stipulare atti giuridici, laddove gli stessi perseguano il loro interesse superiore. Le ricadute operative che questo approccio comporta nell'ambito dell'analisi delle misure di contemperamento delle vulnerabilità dei minori nella dimensione digitale sono molteplici ⁽¹⁷⁹⁾.

Ciò che preme in questa sede evidenziare al fine di cogliere elementi di *common core* e *better rule* capaci di circolare tra diversi sistemi di tutela è, da un lato, il carattere obbligatorio dell'introduzione di meccanismi di accertamento dell'età e, dall'altro, l'equiparazione del trattamento dei dati personali dei minori di età al regime previsto per i dati sensibili. Inoltre, come osservato per il DSA europeo, ai fornitori di prodotti e servizi *online* è vietato utilizzare processi decisionali automatizzati per finalità di *marketing* rivolto direttamente ai minori di età ⁽¹⁸⁰⁾. Questi elementi, oltre ad essere comuni ad altri sistemi giuridici, ben si prestano ad essere utilizzate l'una per segnare l'ambito di applicazione delle misure di protezione attivate nella dimensione digitale e l'altra per fornire una chiave di lettura nota delle caratteristiche che il sistema di tutela deve possedere ⁽¹⁸¹⁾.

9.3. *Il Digital Personal Data Protection Act indiano.*

Con una tecnica legislativa diversa rispetto a quella illustrata per la Cina, anche il sistema indiano impone agli operatori economici una verifica dell'età dell'utente digitale per poi applicare ai dati dei minori

⁽¹⁷⁹⁾ Si consideri che anche in Cina la maggiore età coincide con il compimento di diciotto anni. Per un approfondimento sulle misure tecnico-organizzative di salvaguardia per i minori si rinvia al prossimo capitolo, *infra* Cap. 2 §3.3.

⁽¹⁸⁰⁾ Il sistema di tutele per i minori di età disegnato in Cina prevede tre linee di intervento: la promozione dell'acquisizione di conoscenze e competenze per la dimensione digitale, il monitoraggio a fini di prevenzione circa l'esposizione a contenuti nocivi (per la salute, per lo sviluppo di dipendenze, per l'istigazione a violenza, odio, cyberbullismo, sfruttamento delle vulnerabilità a fini commerciali) e controllo efficace delle informazioni di carattere personale, G. ZHENG, J. SHU, *In the name of protection—A critical analysis of China's legal framework of children's personal information protection in the digital era*, in *Computer Law & Security Review*, Volume 53, 2024, 105979, <https://doi.org/10.1016/j.clsr.2024.105979>.

⁽¹⁸¹⁾ LI, WENLONG, J. CHEN, *From Brussels Effect to Gravity Assists: Understanding the Evolution of the GDPR-Inspired Personal Information Protection Law in China*, in *The Computer Law and Security Report* 54 (2024): 105994.

di età un regime speciale, avente le medesime caratteristiche di quello che disciplina i dati sensibili. Il Digital Personal Data Protection Act ⁽¹⁸²⁾ del 2023, infatti, dedica una intera norma al trattamento dei dati dei minori di età, coniugando alcuni profili di *due diligence* per gli operatori economici non presenti in altre normative sulla *privacy*: all'art. 9 stabilisce che il titolare del trattamento, prima di processare dati concernenti una persona che non abbia compiuto diciotto anni, o un soggetto disabile, debba assicurarsi che ci sia un legale rappresentante che presti un consenso verificabile ⁽¹⁸³⁾. Ciò impone a ogni organizzazione di introdurre sistemi di verifica dell'età degli utenti, procedendo ad una sostanziale equiparazione di meccanismi di tutela per le due categorie di soggetti vulnerabili: disabili e minori di età.

La medesima norma stabilisce, inoltre, che lo stesso titolare del trattamento garantisca l'assenza di rischi in termini di probabilità che l'elaborazione di dati personali possa essere pregiudizievole per il benessere del bambino. In altri termini, con un risultato analogo a quanto osservato per l'Online Safety Act britannico, il trattamento non solo non deve recare pregiudizio al bambino, in termini di incolumità, sicurezza, e salute, ma deve essere tale da non poter nemmeno com-

⁽¹⁸²⁾ Digital Personal Data Act, 11.08.2023, n. 22, <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>. Per un commento, si veda P. NAITHANI (2024), *Analysis of India's Digital Personal Data Protection Act, 2023*, in *International Journal of Law and Management*, <https://doi.org/10.1108/IJLMA-05-2024-0174>, sui lavori preparatori l'influenza del GDPR è evidente, si parla di "*regulatory transplants in the Indian context*", così M. DEVA PRASAD - C. SUCHITHRA MENON, *The Personal Data Protection Bill, 2018: India's Regulatory Journey towards a Comprehensive Data Protection Law*, 28 *International J.L. & Info. Tech.* 1 -19 (Spring 2020), per segnalare quale approccio normativo sia stato adottato dalla Committee of Experts on Data Protection a valle della decisione della Corte Suprema pubblicata nel 2017 *Justice K.S. Puttaswamy v Union of India* (C) 494/2012), che aveva sancito il diritto alla privacy e riservatezza. Nel rapporto della Commissione di esperti chiamata a disegnare i confini della strategia digitale indiana emerge che l'identificazione di disposizioni specifiche a tutela dei minori di età costituisce un risultato della consultazione pubblica avviata a seguito della pubblicazione del precedente *White Paper of the Committee of Experts on A Data Protection Framework for India*, Ministry of Electronics and Information Technology, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, p. 27, accessed 14 November 2024.

⁽¹⁸³⁾ All'articolo 2 introduce la definizione di "*data principal*", ovvero soggetto interessato, ruolo che può essere assunto anche dal genitore o dal legale rappresentante del minore, nel caso in cui il trattamento riguardi dati concernenti un minore di età.

prometterne il superiore interesse del bambino, che si traduce tanto nella protezione da rischi e pericoli, quanto nella promozione delle opportunità offerte dalla specifica attività di trattamento di dati personali. Calando la norma nell'ambito dei meccanismi di identificazione e mitigazione dei rischi di un determinato trattamento, notiamo che la formula utilizzata che richiama il concetto di probabilità, di fatto, implichi che l'assenza di rischi sia frutto di una valutazione di impatto ad opera del titolare chiamato ad escludere la permanenza di qualsivoglia rischio residuale per i bambini dalle attività di trattamento proposte. La questione appare di complessa attuazione dal momento che escludere *in toto* la probabilità che una attività di trattamento *in fieri* possa produrre dei rischi nella sfera di interessi degli utenti nella dimensione digitale appare complicato da sostenere. Si tratta invero dello stesso parametro adottato dal legislatore europeo per la valutazione della violazione di dati ai sensi dell'art. 33 GDPR, con la differenza che l'analisi in questo caso non è prognostica, ma attuale: per cui il titolare può escludere la probabilità che una certa violazione di dati abbia causato una compromissione dei diritti e delle libertà della persona al fine di valutare se procedere o meno alla notifica all'autorità garante.

Tornando all'analisi del sistema indiano, sempre l'art. 9 introduce un divieto che nella sensibilità del legislatore europeo si è reso manifesto nel DSA con il divieto di *targeting* pubblicitario. Infatti, si proibisce, salvo eccezioni che siano espressamente previsti, il tracciamento, o il monitoraggio comportamentale, o la pubblicità mirata rivolti ai bambini. Dei contemperamenti sono applicati a certi titolari di trattamento nell'ambito di un regime di esenzioni che possono riguardare i trattamenti di dati effettuati su soggetti sopra determinate fasce d'età, laddove sia stata data evidenza e garanzia delle modalità "*verificabilmente sicure*" delle operazioni sui dati effettuate. In ogni caso, tali esenzioni sono oggetto di notifica da parte del Governo Centrale ⁽¹⁸⁴⁾.

⁽¹⁸⁴⁾ Si tratta dei *Significant Data Fiduciary*, che in ragione del volume e natura dei dati, dei rischi e impatto dei trattamenti per la sovranità e integrità dell'India o per la democrazia elettorale o per la sicurezza e ordine pubblico sono sottoposti ad un regime più stringente dal punto di vista organizzativo, dovendo — a desempio — nominare un *data protection officer*, svolgere *audit* periodici di sicurezza, implementare *policy* di *data breach* e procedere ad espletare attività di reportistica periodica. In dottrina: D. SHARMA, L. BHAGAT, S. SHARMA, *Regulating Children's Personal Data Protection in India: No Child's Play*. Development (2024). <https://doi.org/10.1057/s41301-024-00402-w>.

A fini di attuazione, la parte dedicata alle sanzioni per la mancata conformità agli obblighi previsti dalla normativa specifica aggravamenti laddove le violazioni siano riferite alla disposizione illustrata posta a tutela dei minori di età.

Rispetto all'innovazione tecnologica anche l'India — come il Giappone — si colloca fra quegli ordinamenti che hanno adottato una strategia per l'IA inclusiva, identificando — in particolare — alcune aree per interventi mirati a potenziare le infrastrutture e l'accesso ai sistemi informativi, corredata dal 2021 dall'enunciazione di principi *ad hoc* per un uso responsabile dei sistemi di IA, che richiamano i sette requisiti sviluppati nell'ALTAI *checklist*. In questo caso nessun riferimento specifico ai minori di età, appare essere introdotto come meritevole di menzione ⁽¹⁸⁵⁾.

I sistemi asiatici analizzati offrono alla riflessione comune la condivisa necessità di inquadrare il sistema di tutele per l'utente digitale minorenne nell'ambito di forme di protezione già esplorate per altre manifestazioni di vulnerabilità (come la parificazione al regime giuridico dei dati sensibili), ovvero volte a rendere effettivo l'istituto della rappresentanza dell'esercente le responsabilità genitoriali. Dall'altro lato, si osserva che — per quanto concerne la regolamentazione dell'innovazione tecnologica — è elemento comune il mantenimento di un approccio basato su principi informativi di carattere generale. Il che manifesta una attuale immaturità a ritagliare specifiche linee di indirizzo per i minori di età, ma allo stesso tempo l'atteggiamento dei legislatori nell'ambito della datificazione ben fa presumere che i giovani utenti non saranno trascurati una volta che sarà presa l'iniziativa regolatoria in materia.

10. Le strategie a portata di bambini e adolescenti nei sistemi sudamericani.

I sistemi sudamericani ben si prestano all'esercizio di comparazione rispetto alle iniziative europee, in quanto sono frutto della

⁽¹⁸⁵⁾ National Strategy For Artificial Intelligence, #AIFORALL, <https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policy-initiatives-24951>.

circolazione del modello europeo ⁽¹⁸⁶⁾, dal quale mutua alcune linee di indirizzo adattandole alla normativa pre-esistente e al dibattito locale. L'influenza della strategia europea dei dati è infatti dichiarata nelle relazioni che presentano proposte legislative dei sistemi sudamericani ⁽¹⁸⁷⁾. Si rinvencono, tuttavia, alcune rilevanti differenze, soprattutto con riferimento alla tecnica legislativa adottata e rispetto alle metodologie per la mitigazione dei rischi della società dell'informazione e la promozione delle opportunità emergenti dalla transizione digitale di beni e servizi.

Di particolare interesse appare l'attenzione prestata al bilanciamento tra autonomia decisionale degli adolescenti rispetto alle esigenze di protezione dei bambini, cui corrisponde, in alcuni casi, anche la connotazione di informazioni sensibili con le relative conseguenze in ordine alle basi giuridiche che ne giustificano il trattamento ⁽¹⁸⁸⁾.

10.1. (Segue). Perù.

Nel sistema peruviano, ad esempio, è stata promulgata una legge sull'uso dell'IA ⁽¹⁸⁹⁾ che consta di soli cinque articoli e che si pone

⁽¹⁸⁶⁾ Nell'esercizio di comparazione appare interessante riprendere le osservazioni sul rapporto tra "contaminazione" e "stingimento" derivanti dalla circolazione dei modelli (cfr. A. MIRANDA, *Lo "stingimento" delle regole giuridiche tra diritti e limiti nell'era dei flussi migratori e della crisi delle nazioni*, Cardozo El. Law Bull, 2018, p.1 ss.), considerando il ruolo di "prestigio" che il legislatore UE ha assunto in materia di dati attraverso l'imposizione di meccanismi di adeguamento ai principi enunciati nel Regolamento UE 2016/679 per i flussi transfrontalieri e la componente di "influenze reciproche" che determinano l'evolversi di un diritto ibrido, sul punto N. FOSTER, *Introduction to "A Fresh Start for Comparative Legal Studies? A Collective Review of Patrick Glenn's Legal Traditions of the World"*, in Journal of Comparative Law, 2006, p. 100 ss.

⁽¹⁸⁷⁾ W. DE SANTANA, A. L. Y ARCHEGAS, J. GABRIEL, *La protección de niños y adolescentes en las plataformas digitales: Avances en el tema en Brasil*. Agenda Estado de Derecho, 2023/12/20, in <https://agendaestadodederecho.com/la-proteccion-de-ninos-y-adolescentes-en-las-plataformas-digitales-avances-en-brasil/>. P.R. FLORES CEDENO, C.R. LÓPEZ PAZ, *Government Management of Information Technology in the Latin American Context. Salud*, in Ciencia y Tecnología. 2024 Jan. 1,3:682, A. -MUÑOZ-DEL-CARPIO-TOIA ET AL, *Protección de Datos de Salud: El Reto de La Armonización Legislativa En América Latina*, Revista del Cuerpo Médico del Hospital Nacional Almanzor Aguinaga Asenjo 16.2 (2023).

⁽¹⁸⁸⁾ Su cui *infra*.

⁽¹⁸⁹⁾ Ley 31814/2023, *Ley que promueve el uso de la Inteligencia Artificial (IA) en favor del desarrollo económico y social del país*. Si veda il contributo di J.J.

l'obiettivo di garantirne un uso “*etico, sostenibile, trasparente, replicabile e responsabile*”. In particolare, si enunciano i principi informatori della materia (art. 1), tra cui: sicurezza, coinvolgimento dei soggetti interessati nei processi decisionali volti a regolamentare le diverse applicazioni, digitalizzazione, responsabilizzazione e approccio etico, tutela della *privacy* e si elencano poi gli interessi nazionali (art. 2) sottesi alla promozione delle nuove tecnologie e dei sistemi digitali per il miglioramento dei servizi pubblici e privati nei settori chiave dell'economia del paese (istruzione, trasporto, sicurezza digitale, inclusione, difesa, etc).

Si forniscono delle definizioni di intelligenza artificiale, sistema di intelligenza artificiale, tecnologia emergente e algoritmo (art. 3) e si istituisce una autorità tecnico-normativa (art. 4) con compiti di coordinamento, valutazione e supervisione rispetto all'uso e alla promozione dello sviluppo dell'intelligenza artificiale e delle tecnologie emergenti.

L'iniziativa va letta in combinato disposto con le disposizioni contenute nella legge sulla protezione dei dati personali peruviana, risalente al 2011, e il relativo regolamento attuativo al 2013 ⁽¹⁹⁰⁾. Quest'ultimo dedica un capitolo ai bambini e agli adolescenti, stabilendo che il trattamento dei dati personali dei minori sia subordinato al consenso del legale rappresentante (art. 27), salvo che il minore abbia compiuto anni quattordici “*a condizione che le informazioni fornite siano state espresse in un linguaggio da loro comprensibile*” e fatti salvi i casi in cui sia espressamente prevista l'assistenza del genitore (art. 28). La stessa norma esclude che il consenso al trattamento dei dati personali possa dare accesso a servizi e beni riservati ad adulti. Questa specificazione rileva notevolmente per le riflessioni che abbiamo sviluppato nei paragrafi precedenti, in quanto delinea per il sistema

YAIPIÉN-TORRES - V.W. ROJAS-LUJÁN, *Ética Jurídica En La Interpretación de Normas Legales Con Inteligencia Artificial*, *Revista Arbitrada Interdisciplinaria Koinonía* 9.18 (2024): 147—164.

⁽¹⁹⁰⁾ Ley 29773/2013, *Ley de Protección de Datos Personales*, <https://www.leyes.congreso.gob.pe/Documentos/Leyes/29733.pdf>, Reglamento de la ley n. 29733, Decreto Supremo 003-2013-Jus, <https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779>. V. QUISPE - C. DENNIS, *Derecho e Inteligencia Artificial En El Mundo de Hoy: Escenarios Internacionales y Los Desafíos Que Representan Para El Perú*, *Thémis* 79 (2021): 311-322, G. MIGUEL RECIO, *Nivel Adecuado Para Transferencias Internacionales de Datos*, *Derecho PUCP* 83 (2019): 207-240.

peruviano un confine ben saldo tra capacità di discernimento a fini contrattuali e quella per acconsentire al trattamento di dati personali. A questo proposito, tuttavia, emerge un profilo di criticità in ordine all'applicabilità di questa norma alla dimensione digitale, essendo stata concepita per i rapporti nella dimensione reale e sussistendo a protezione dei minori di età *online* il solo regime di tutela penalistico, rafforzato peraltro nel 2023, senza nulla aggiungere in ordine ai rapporti fra privati ⁽¹⁹¹⁾.

La struttura asciutta e di rinvio della Ley n. 31814/2023 sull'enunciazione di principi in materia di nuove tecnologie e IA non si presta a colmare lacune sistemiche. Sarebbe stato più opportuno, magari, procedere all'approvazione di un regolamento applicativo, che declinasse i principi in meccanismi di tutela dei soggetti interessati, ovvero che articolasse gli interessi nazionali cogliendo le vulnerabilità emergenti dall'innovazione tecnologica, chiarendo — per esempio — il rapporto tra normative di settore, come la possibilità di applicare le misure indicate dalla normativa sulla protezione dei dati alla tutela della posizione dei minori di età alla dimensione digitale.

10.2. (Segue). *Argentina*.

Uno sforzo sistematico più robusto si apprezza, invece, nelle prospettive di *de iure condendo* in discussione in Argentina, che si appresta ad approvare una proposta di modifica alla legge sulla protezione dei dati personali ⁽¹⁹²⁾ per adeguarla all'innovazione tecnologica e all'impatto sulle informazioni personali, specialmente per quelle sensibili.

La proposta di modifica introduce alcune misure a tutela dei bambini e degli adolescenti, prevedendo la soglia del compimento del tredicesimo anno di età per esprimere un consenso valido. L'articolo 18 della proposta specifica, da un lato, che il titolare del trattamento debba “*compiere sforzi ragionevoli per verificare*” la validità del consenso prestato dal minore o dal legale rappresentante nel caso di infratredicenne; dall'altro lato, che non possono essere raccolti dati

⁽¹⁹¹⁾ Ejecutivo publicó el Decreto Legislativo n. 1591 del 2023.

⁽¹⁹²⁾ Ley 25.326, *Ley de Protección de los Datos Personales*, 4 ottobre 2000, v. M. BASTERRA, *El HáBeas Data: La Reforma Constitucional de 1994 y La Sanción de La Ley 25.326; de Protección de Datos Personales y de HáBeas Data*, *Dikaion* 10 (2009).

ulteriori a quelli strettamente necessari applicazioni destinate ai minori stessi, come giochi, applicazioni internet, o altre attività.

A tal proposito, si introduce una specifica condizione di liceità per il trattamento di dati sensibili dei minori e degli adolescenti oltre al consenso, ovvero il fatto che lo stesso sia “*indispensabile per l'interesse pubblico o per salvaguardare la vita propria o di terzi*” ⁽¹⁹³⁾.

Considerando che le basi giuridiche per il trattamento di dati sensibili secondo la normativa argentina — al pari del GDPR — sono giustificate anche in presenza di altre condizioni, la formulazione appare restringere la rosa per questa particolare categoria di soggetti interessati. Occorre, dunque, domandarsi quale bilanciamento debba operarsi nel caso in cui l'interessato, minore di età, si trovi a ricoprire posizioni nella società che abilitino trattamenti dei relativi dati sensibili nelle condizioni descritte dalle altre basi giuridiche, che l'art. 16 della proposta enuncia: ad esempio, in caso di necessità di osservare la normativa sindacale e a tutela dei lavoratori (lett. g), in quanto minore lavoratore, o laddove quest'ultimo sia oggetto di prestazioni nell'ambito di attività di assistenza umanitaria (lett. i). Appare difficile negli esempi escluderne la liceità del trattamento di dati sensibili dei minorenni e dover ricorrere alla base giuridica del consenso. Sarebbe stato preferibile, pertanto, formulare un coordinamento diverso tra l'art. 18, *lex specialis* rispetto alle disposizioni generali di cui all'art. 16, imponendo ai titolari di operare una valutazione in ordine al carattere indispensabile del flusso di informazioni sensibili che riguardano bambini e adolescenti, evitando di mettere in dubbio la natura autonoma delle altre basi giuridiche.

Innovativa e particolarmente coerente, invero, con gli obiettivi della proposta di promuovere una datificazione della società anche a portata di minori di età, si colloca un'altra misura organizzativa prevista dall'art. 18, comma 6.

Si tratta dell'attribuzione allo Stato e alle istituzioni scolastiche del compito di “*informare e formare i minori e gli adolescenti sui possibili rischi ai quali sono esposti*”, per un “*uso responsabile e sicuro*” delle informazioni personali, soprattutto con riferimento alla loro circolazione e condivisione. La formulazione del comma orienta le competenze e conoscenze da acquisire in termini di educazione digitale per i

⁽¹⁹³⁾ La formula richiama le basi giuridiche di cui all'art. 9 GDPR, comma 2, lettere a), c) e g), richiamate dall'art. 16 della proposta legislativa argentina con una numerazione diversa.

minori di età, rispetto — in particolare — al diritto alla riservatezza, all'autodeterminazione informativa, in allineamento con le caratteristiche dell'informativa espresse nei commi precedenti ⁽¹⁹⁴⁾ e al rispetto dei diritti degli altri. Quest'ultima accezione si presta a racchiudere ogni forma di prevenzione rispetto a fenomeni di abuso o uso improprio delle informazioni: dal cyberbullismo, ai contenuti che minano l'incolumità fisica o psichica delle persone, alla misinformazione, etc. Di conseguenza, le istituzioni sono chiamate ad intervenire direttamente nella costruzione di percorsi formativi e canali di sensibilizzazione al fine di rafforzare la consapevolezza dei giovani utenti e renderli, pertanto, capaci di gestire il flusso delle proprie informazioni nella dimensione digitale in maniera sicura e responsabile. Questo profilo apre la strada, come vedremo nei prossimi capitoli, alla progettazione di percorsi standardizzati — almeno al livello nazionale — al fine di incrementare le competenze e capacità di controllo di una intera generazione, come misura complementare alle attività di conformità e *due diligence* che gli operatori dei servizi digitali devono implementare a tutela degli utenti consumatori minorenni.

Il sistema argentino si prepara ad introdurre meccanismi robusti e lungimiranti rispetto alle evidenze della letteratura in materia, coinvolgendo operatori economici, istituzioni, utenti minorenni e le loro famiglie in forme di cooperazione apprezzabili, suscettibili di essere mutate da altri ordinamenti.

10.3. (Segue). *Il sistema di tutele in Brasile e la risoluzione "settoriale" (cenni e rinvio).*

Anche il sistema di tutele che emerge dalle normative di settore in Brasile introduce alcuni elementi particolarmente efficaci per operare un bilanciamento tra i meccanismi di protezione dei bambini e la graduale autonomia che viene (e deve essere) acquisita dagli adolescenti.

L'art. 14 della legge sulla protezione dei dati personali n. 13.709/

⁽¹⁹⁴⁾ I titolari del trattamento dovranno fornirla “*in modo semplice, chiaro ed accessibile, tenendo conto delle caratteristiche fisico-motorie, percettive, sensoriali, intellettive e mentali dell'utente, con l'utilizzo di risorse audiovisive, se del caso (...) e adeguati alla comprensione del minore o adolescente*”, M. BIBIANA NIETO, *El Sharenting y Los Derechos Personales Simos Del Niño En Argentina, Perspectivas de las ciencias económicas y jurídicas (En línea)* 11.2 (2021), 2021-07, Vol. 11 (2).

2018 ⁽¹⁹⁵⁾ apre la terza sezione della normativa, dedicata ai bambini e agli adolescenti, enunciando come principio informatore la necessità che qualsiasi trattamento debba realizzare il loro interesse superiore. La formula non è meramente di stile, ma ha una rilevanza sostanziale, volta a distinguere misure di salvaguardia diversificate rispetto alle due sotto-categorie di utenti minorenni che, esprimendo bisogni e livelli di maturità altrettanto differenti, richiedono misure adeguate e appropriate affinché siano efficaci ⁽¹⁹⁶⁾. Di conseguenza, le disposizioni contenute nella predetta sezione pongono limiti alle basi giuridiche del trattamento dei dati dei bambini prevedendo, ad esempio, come condizione di legittimità il consenso espresso del genitore o del legale rappresentante (§2), ovvero autorizzando in mancanza solo se “(i) *sia necessario contattare i genitori o i tutori legali*; o ii) *per la protezione del minore*”, specificando che, anche in queste ipotesi, restano vietati la conservazione, il riuso e la condivisione delle informazioni processate.

La norma pone non pochi problemi interpretativi, infatti, anche in questo caso occorre valutare se il legislatore abbia voluto ampliare le maglie della base giuridica del consenso del legale rappresentante relativamente al trattamento dei dati dei soli bambini e non anche per quelli relativi agli adolescenti. L'interpretazione sarebbe corroborata dal dato letterale che menziona gli adolescenti nell'*incipit* della sezione e non nei diversi paragrafi della disposizione. La collocazione risulta coerente con l'equiparazione delle informazioni riguardanti i (soli) bambini allo statuto giuridico dei dati sensibili, limitando — di fatto — la possibilità di abilitare flussi di dati riguardanti questi ultimi in virtù delle altre basi giuridiche menzionate nell'art. 7 (ad esempio il contratto, l'adempimento di una obbligazione per il titolare del trattamento, etc), che sarebbero funzionali al compimento di atti giuridici che i soli adolescenti — a certe condizioni — potrebbero porre in essere anche senza rappresentanza legale. Una argomentazione contra-

⁽¹⁹⁵⁾ Ley General de Protección de Datos Personales, Ley 13.709/2018, https://www.dataguidance.com/sites/default/files/lgpd_translation.pdf, in dottrina: C. RODRIGUES DA SILVEIRA - C. KARPINSKI, *Diplomática Contemporânea No Atendimento Aos Principios Da Lei Geral de Proteção de Dados*, *Brazilian Journal of Information Science* 17.17 (2023), F. FRANCYELCYO PUSSI - R. BARROS, *LGPD - From Theory to Practice*, 2022 *17th Iberian Conference on Information Systems and Technologies (CISTI)* (2022): 1-6.

⁽¹⁹⁶⁾ In particolare, si richiama l'art. 2 dello statuto dell'infanzia e dell'adolescenza, Ley n. 8.069, del 13 luglio 1990, che prevede che sia considerato bambino la persona fino ai dodici anni e adolescente quella tra i dodici ed i diciotto anni, https://www.planalto.gov.br/ccivil_03/leis/l8069compilado.htm.

ria a questo orientamento interpretativo, invero, potrebbe fare leva sulla prevalenza del principio di interesse superiore, in ragione del quale le eccezioni allo scenario normato sarebbero sempre giustificate caso per caso. Tuttavia, al paragrafo 5 dello stesso articolo, si richiamano le attività di trattamento descritte dal paragrafo 1, ponendo come regola di diligenza richiesta ai titolari del trattamento il compimento di “*sforzi ragionevoli*”, considerate le tecnologie disponibili, rispetto alle attività di verifica della validità del consenso espresso dal genitore.

Sempre all’art. 14 trova declinazione un principio noto al GDPR: quello di minimizzazione, che (come osservato nella proposta argentina) si applica rispetto al conferimento di dati per l’utilizzo di giochi, *internet* e altre attività in termini di divieto per il titolare di raccogliere dati non strettamente necessari al relativo uso.

Infine, rispetto al principio di trasparenza, nel prevedere che l’informativa *privacy* debba essere appropriata alla comprensione del minore, sebbene rivolta alla raccolta del consenso del genitore, il paragrafo 6, della medesima norma, specifica la necessità che siano presi in considerazione per opportuni adattamenti rispetto alle risorse da utilizzare (ad esempio audiovisive), anche “*aspetti fisico-motori, percettivi, caratteristiche sensoriali, intellettuali e mentali dell’utente*”. La norma esprime una particolare sensibilità rispetto alla varietà di situazioni che possono costituire barriere alla comprensione delle informative, individuando profili che ben potrebbero formare una buona prassi nelle interpretazioni delle formule utilizzate nelle altre legislazioni allorquando si riferiscono alla necessità che il linguaggio utilizzato sia chiaro e alla effettiva portata del soggetto interessato /utente.

La stessa attenzione emerge anche nel disegno di legge n. 2628/2022 ⁽¹⁹⁷⁾, che mira ad andare oltre la tutela penale contro i crimini digitali — peraltro integrata recentemente con l’introduzione di una

(197) Projeto de Lei n. 2628, de 2022, *Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais*, <https://www25.senado.leg.br/web/atividade/materias/-/materia/154901>. I. GÓMEZ FERNÁNDEZ, *Posição Jurídica de Crianças e Adolescentes Em Ambientes Digitais: Posição jurídica de crianças e adolescentes em ambientes digitais*, *Espaço Jurídico* 2 (2022): 239-258; R. BÔAS - V. VILLAS DE PINHO, C. COSTA, R. RODRIGUES, *Efetividade da tutela coletiva na proteção de direitos de crianças e adolescentes no ambiente digital*, *Revista Argumenta*. 2023(41):127-152. <https://www.proquest.com/scholarly-journals/efetividade-da-tutela-coletiva-na-proteção-de/docview/3069282269/se-2>.

fattispecie autonoma di reato relativa al cyberbullismo ⁽¹⁹⁸⁾ — che dispone misure atte a garantire i diritti dei minori di età rispetto a qualsiasi prodotto o servizio tecnologico della società dell'informazione cui bambini e adolescenti possono accedere.

I proposti meccanismi di tutela del minorenne-utente-consumatore del servizio digitale si sviluppano su una pluralità di livelli (articolo 7): il primo muove dalla necessità di proteggere l'integrità degli utenti bambini e adolescenti. Un secondo livello riguarda la necessità di garantire l'assoluta prevalenza dei relativi interessi. In questa prima distinzione emerge il binomio protezione-promozione che si traduce nel processo di valutazione dei rischi in misure di mitigazione e incentivi per garantire l'accesso e sfruttamento delle opportunità della dimensione digitale.

Il terzo livello si concentra sulla peculiarità degli utenti che versino nella “*condizione peculiare di una persona in via di sviluppo biopsichico*”, facendo emergere la necessità di adeguare le azioni di protezione-promozione a diverse fasce di età rappresentate dalla categoria. Il quarto riguarda la necessità di garantire “*sicurezza contro intimidazioni, sfruttamento, abusi, minacce e altre forme di violenza*” che, letto in combinato disposto con il quinto piano di analisi, ovvero il “*rispetto dell'autonomia e del progressivo sviluppo dell'individuo*”, copre gli usi impropri dell'ambiente digitale, come espresso nella omologa proposta argentina. Il sesto (ed ultimo) livello è quello relativo alla tutela contro “*l'indebito sfruttamento commerciale*”, che si declina attraverso la garanzia della “*inviolabilità delle immagini, dei suoni e di altre informazioni acquisite, archiviate e trasmesse a genitori o tutori*” attraverso meccanismi di monitoraggio e profilazione attivati in prodotti o servizi destinati all'infanzia ⁽¹⁹⁹⁾.

In questa prospettiva, la proposta di legge indica numerose misure tecniche e organizzative da introdurre a seconda del servizio o prodotto reso accessibile ai minori di età. Ad esempio, l'art. 8 vieta le cc.dd. *loot box*, in quanto considerate alla stregua del gioco d'azzardo ⁽²⁰⁰⁾. L'art.

⁽¹⁹⁸⁾ Lei n. 14.811/2024 che modifica il codice penale introducendo i delitti di bullismo e cyberbullismo.

⁽¹⁹⁹⁾ L'ultimo comma dell'art. 7 introduce un monito affinché lo sviluppo e l'uso di meccanismi di monitoraggio siano guidati dall'interesse superiore del minore considerando lo sviluppo progressivo delle relative capacità.

⁽²⁰⁰⁾ Si tratta di scatole misteriose di contenuti digitali nei videogiochi (come vantaggi od oggetti cosmetici), che i consumatori acquistano con denaro reale senza

9 stabilisce che laddove sia prevista una interazione sincrona o asincrona con minori di età attraverso messaggi di testo, audio o video, siano introdotte delle misure tecniche che limitino la stessa alla fascia di età più restrittiva, chiedendo al Ministero della giustizia un intervento per regolamentarne i dettagli; si prevede, inoltre, la necessità che il sistema si doti di controlli parentali e di meccanismi per riportare abusi e reclami, nonché di provvedere a rendere pubbliche e trasparenti le informazioni relative alle infrazioni, al pari di quanto vedremo nelle esperienze legislative USA e riprese dal DSA europeo.

Rispetto alle forme di *targeting* pubblicitario e pratiche manipolative, l'art. 10 distingue, ancora una volta le due sottocategorie di soggetti minorenni, disciplinando norme diverse quando la comunicazione riguarda bambini, rispetto a quelle rivolte a tutelare gli adolescenti. Nel primo caso, sono valutate le esposizioni di prodotti o servizi, anche gratuiti, considerando contenuti audio, o video, o testi con linguaggio infantile ed effetti speciali, animazioni, uso di personaggi noti, giocattoli, promozione con distribuzione di premi, oppure di omaggi, oggetti da collezione, oppure promozione con concorsi o giochi che attirino il pubblico infantile. Nel secondo caso, la proposta di legge pone l'attenzione sulla necessità che le stesse comunicazioni, che devono esplicitamente indicare che sono pubblicitarie o rese per finalità di *marketing*, non favoriscano alcuna condotta illecita o discriminatoria, né promuovano forme di violenza o degrado ambientale e siano tali da “*non indurre, neppure implicitamente, un sentimento di inferiorità negli adolescenti, se non consumano un determinato prodotto o servizio*”.

Questi correttivi sono ragionevolmente introdotti al fine di mitigare quelle specifiche vulnerabilità cui è esposto un soggetto adolescente che stia acquisendo quotidianamente maggiore autonomia. Apprezzabile lo sforzo armonizzante di mantenere il *discrimen* nel compimento di anni dodici, in allineamento con lo statuto nazionale dei diritti dell'infanzia e adolescenza, abbassando il dato proveniente dall'art. 8 GDPR europeo.

Infine, la proposta include una norma di chiusura, che impone

tuttavia conoscerne l'oggetto o le caratteristiche fino al pagamento. Si veda sul punto il rapporto del Norwegian Consumer Council, *Insert Coin: How the gaming industry exploits consumers using loot boxes*, 2022, <https://storage02.forbrukerradet.no/media/2022/05/2022-05-31-insert-coin-publish.pdf> sul *design* manipolativo associato al *marketing*.

alcuni divieti significativi, tra cui: l'utilizzo di tecniche di profilazione per indirizzare la pubblicità a bambini e adolescenti; l'utilizzo di tecniche volte a riconoscere le emozioni; l'uso della realtà aumentata ed estesa e realtà virtuale a questo scopo.

Queste indicazioni ancora in discussione come legge sono state, invero, recepite nella recentissima risoluzione n. 245/2024 sui diritti dell'infanzia e dell'adolescenza nell'ambiente digitale. L'iniziativa, seppur di rango inferiore, costituisce un *unicum* nel panorama legislativo in quanto si tratta di una prima forma di regolamentazione di settore, dedicata ai bambini e agli adolescenti nello spazio digitale, completa di principi informatori della materia, di riconoscimento di diritti e previsione di obblighi correlati da meccanismi di attuazione.

In particolare, il riconoscimento del diritto alla protezione dei dati ne risulta rafforzato e ad esso si lega un principio di “*autonomia progressiva*” dell'utente ⁽²⁰¹⁾. Si prevedono, infatti, specifici obblighi di protezione, non solo per i legali rappresentanti, ma soprattutto per i fornitori di servizi digitali affinché i contenuti accessibili siano “*compatibili con la condizione del minore di età*”, il che significa effettuare una valutazione di impatto che l'uso della tecnologia può avere sullo “*sviluppo cognitivo, emotivo e sociale dell'individuo*” e fornire indicazioni per i familiari e adulti di riferimento ⁽²⁰²⁾. Tale principio va oltre la valutazione della probabilità di recare nocimento, osservato nelle altre esperienze, e si colloca nell'ambito della promozione dei diritti dei minori come priorità e non in misura sussidiaria rispetto a un sistema di tutele efficiente. In altri termini, la risoluzione brasiliana invita gli operatori e le istituzioni a porre come obiettivo il benessere del minore nella dimensione digitale e senza limitarsi alla mera protezione da eventuali rischi o pericoli.

⁽²⁰¹⁾ V. BARBA, *Autonomia progressiva e miglior interesse della persona minore di età*, in *Dir. succ e fam.*, 2023, p. 441 ss.

⁽²⁰²⁾ Resolução, 5 aprile 2024, dispõe sobre os direitos de crianças e adolescentes em ambientes digitais, <https://perma.cc/37P9-5A23>. Per un primo commento, si veda G. DAMASIO GOULART, *Resolução do Conanda sobre proteção de crianças e adolescentes no meio digital*, 25 aprile 2024, <https://www.conjur.com.br/2024-abr-25/resolucao-do-conanda-sobre-protecao-de-criancas-e-adolescentes-no-meio-digital/>.

11. I sistemi africani: cenni alle misure introdotte in Swaziland, Uganda e Ruanda.

L'interesse verso le legislazioni africane muove dalla necessità di verificare nei paesi in via di sviluppo, in cui gli investimenti per una transizione digitale dei servizi e prodotti sono ridotti, quale sia l'atteggiamento dei legislatori verso le problematiche comuni di protezione e promozione dei diritti dei minori.

Da un lato, si ravvisa la necessità di identificare strumenti per colmare quel divario infrastrutturale che limita, se non esclude, l'accesso a servizi e prodotti digitali e, di conseguenza, alle opportunità per le nuove generazioni di contribuire ai processi economici e di innovazione tecnologica. Dall'altro lato, emerge la consapevolezza che la limitazione delle risorse non solo non esime, ma incrementa l'esposizione dei giovani utenti ai pericoli derivanti dagli strumenti offerti dalla società dell'informazione: vuoi per una ridotta capacità di sicurezza e resilienza dei sistemi, vuoi per una ridotta alfabetizzazione rispetto alle implicazioni dell'uso improprio delle informazioni nello spazio digitale. Per tali ragioni il dibattito sulla regolamentazione dei servizi digitali e delle tecnologie è particolarmente vivace rispetto alla necessità di tutelare l'incolumità fisica e psichica degli utenti minorenni da abusi e usi illeciti ⁽²⁰³⁾.

Oltre al recepimento delle Convenzioni internazionali, alcuni sistemi giuridici africani hanno aderito a convenzioni cc.dd. regionali che si occupano di enunciare principi informatori in materia di datificazione della società. Nell'area della Comunità degli Stati dell'Africa Occidentale (ECOWAS) alcuni strumenti giuridici legati alla sicurezza informatica e lotta alla criminalità informatica sono stati adottati negli ultimi quindici anni ⁽²⁰⁴⁾.

Rispetto ai diritti dei minori di età, accanto alla Carta Africana sui diritti e il benessere dell'infanzia dell'Unione Africana ⁽²⁰⁵⁾, vi è la

⁽²⁰³⁾ JM HUET, *Le digital en Afrique. Les cinq sautes numériques*, Lafon, 2017, più di recente European Investment Bank, *The rise of Africa's digital economy*, 2021, https://www.eib.org/attachments/thematic/study_the_rise_of_africa_s_digital_economy_en.pdf.

⁽²⁰⁴⁾ Legge aggiuntiva del 2 ottobre 2009 relativa alle transazioni digitali nell'area ECOWAS, e quella relativa alla protezione dei dati personali nell'area ECOWAS, nonché la direttiva del 19 agosto 2011 relativa alla lotta alla criminalità informatica nell'area ECOWAS.

⁽²⁰⁵⁾ L'Unione Africana consta oggi di 55 stati membri.

Convenzione africana di Malabo sulla cybersicurezza e la protezione dei dati personali del 17 giugno 2014 ⁽²⁰⁶⁾, che prevede specifiche disposizioni a tutela dei minori *online*. Quest'ultima, oltre a punire la pornografia minorile, introduce delle misure educative, nell'ambito della promozione della cultura della sicurezza. In particolare, l'art. 26 stabilisce che gli Stati possano adottare strategie che includano, oltre a piani per la sicurezza informatica governativa, iniziative e programmi di sensibilizzazione per utenti, piccole imprese, scuole e bambini.

Al livello nazionale, si osserva che trentasei stati africani su cinquantaquattro sono dotati di una regolamentazione per la protezione dei dati e alcune di esse prevedono dei meccanismi di tutela per i minori di età che articolano la protezione oltre le fattispecie penali relative allo sfruttamento e abuso della sfera sessuale.

Si tratta, ad esempio, della legge sulla protezione dei dati personali dello Swaziland del 2022 ⁽²⁰⁷⁾, che nella definizione di dati sensibili include, quelli relativi ai bambini, assieme a quelli genetici, biometrici, giudiziari, etc., limitando pertanto le condizioni di liceità dei relativi trattamenti, nella specie al consenso del legale rappresentante (art. 29). La protezione dei minori, inoltre, costituisce una valida eccezione al divieto di trattare dati relativi alla salute o alla sfera sessuale del soggetto interessato (art. 27, lett. d).

In Uganda, invece, la riforma del 2022 della normativa sull'uso improprio dei computer ⁽²⁰⁸⁾ commina una sanzione pecuniaria, oltre alla reclusione fino a sette anni, in caso di condivisione di dati relativi a un minore di età, senza l'autorizzazione dei legali rappresentanti.

In Ruanda, la legge sulla protezione dei dati personali e sulla vita

⁽²⁰⁶⁾ *Convention de l'Union Africaine sur la cybersécurité et la protection*, 27 giugno 2014, definisce un “quadro normativo appropriato corrispondente all'ambiente giuridico, culturale, economico e sociale africano” nella società dell'informazione. Al momento, è stata sottoscritta da sedici paesi e da tredici, <https://www.afapdp.org/archives/2701>.

⁽²⁰⁷⁾ Data protection Act, 4 marzo 2022, <https://www.esccom.org.sz/legislation/DATA%20PROTECTION%20ACT.pdf>.

⁽²⁰⁸⁾ Computer Misuse (Amendment) Act, 14 ottobre 2022, che aggiorna il precedente del 2011 alla luce dei progressi tecnologici, disponibile <https://www.loc.gov/item/global-legal-monitor/2023-01-05/uganda-computer-misuse-amendment-act-enacted/>.

privata è del 2021 ⁽²⁰⁹⁾. L'art. 9 si occupa interamente del trattamento dei dati di minori di anni sedici, prevedendo come condizione di liceità il consenso del legale rappresentante, purché espresso nell'interesse superiore del bambino. In mancanza di consenso, occorre che il trattamento dei dati dell'interessato minore di età sia giustificato dal perseguimento di un interesse vitale dello stesso ⁽²¹⁰⁾.

Gli esempi riportati consentono di mettere a sistema meccanismi di protezione per i minori di età, soprattutto in contesti dove il processo di transizione digitale di servizi e prodotti è a uno stadio meno avanzato, cionondimeno l'esposizione a rischi e pericoli derivanti dall'accesso e uso improprio delle tecnologie e dell'ambiente digitale può portare alle medesime conseguenze pregiudizievoli per i soggetti esposti a condotte illecite da parte di utenti adulti, ovvero di coetanei.

Per tale ragione anche le misure di mitigazione dei rischi introdotte nei sistemi analizzati si pongono in piena armonia con quelle identificate in ordinamenti ove la rivoluzione tecnologica e digitale appare ad uno stadio più avanzato rispetto all'economia del paese. Ciò corrobora, come vedremo, la posizione per cui la dimensione digitale non crea nuovi diritti, ma articola in modo diverso il principio degli interessi superiori dei bambini e degli adolescenti, la cui tutela dall'esposizione a rischi, comuni e globali, varia in ragione di fattori culturali, oltre che tecnici, e legati allo specifico scenario applicativo. Non è un caso che il bisogno di formare ed essere formati sui rischi e sulle opportunità appaia condiviso in tutte le esperienze analizzate e costituisca una premessa essenziale per poter costruire ambienti digitali e tecnologie non solo sicuri, ma a portata di bambini.

⁽²⁰⁹⁾ Loi n° 058, 2021 del 13 ottobre 2021 relativa alla protezione dei dati personali carattere personale e alla vita privata, https://cyber.gov.rw/fileadmin/user_upload/NCSA/Documents/Laws/OG_Special_of_15.10.2021_Amakuru_bwite.pdf.

⁽²¹⁰⁾ L'agenzia nazionale di sicurezza informatica, molto attiva sul territorio, ha pubblicato un piano strategico 2024-2029 in cui si impegna a promuovere attività di sviluppo di conoscenze e competenze in materia di cybersicurezza anche per bambini e delle linee guida per genitori al fine di promuovere un ambiente online sicuro, <https://cyber.gov.rw/updates/article/7-tips-for-parents-and-guardians-to-keep-children-safe-online/>.

12. Regolamentare la società dell'informazione e le nuove tecnologie per i minori di età: osservazioni di sintesi.

In questo primo capitolo abbiamo elaborato il quadro normativo applicabile alla società dell'informazione e all'innovazione tecnologica, mappando ed evidenziando per ciascuna iniziativa analizzata la presenza o meno di espliciti riferimenti alla tutela dei minori di età. Abbiamo osservato come l'attenzione verso gli utenti minori di età nelle iniziative legate alla digitalizzazione dei sistemi non dipenda dallo stato di avanzamento dei processi di transizione digitale dei servizi e dei prodotti nei diversi sistemi giuridici.

Le ricadute in termini di responsabilità verso gli utenti più deboli, infatti, sono avvertite dai legislatori di ogni rango: dalle Convenzioni di diritto internazionale, che ammoniscono gli Stati Membri affinché i diritti dei minori di età siano attuati nello spazio digitale e al cospetto delle nuove tecnologie, coinvolgendo tutti gli attori rilevanti; al livello di fonte primaria nazionale e sovranazionale in cui a seconda del settore economico spetta agli operatori in ragione del ruolo assunto rispetto alla posizione giuridica del minore di età — *i.e.* titolari del trattamento, prestatori di servizi digitali, sviluppatori, *deployer* o fornitori di sistemi — valutare come implementare le misure di salvaguardia rispetto ai rischi identificati per la specifica applicazione.

A ciò si aggiungono le misure di *soft law* (linee guida, raccomandazioni, risoluzioni) che invero accompagnano tutti — persone giuridiche pubbliche o private o persone fisiche, inclusi gli adulti di riferimento (dai genitori, agli educatori) e i *policy maker* — a rendere effettiva la formula di protezione degli utenti minorenni, attraverso gli strumenti noti alla normativa generale sulla protezione dell'infanzia.

Da questa prima ricostruzione si deducono alcuni elementi particolarmente rilevanti per la nostra riflessione, suscettibili di disegnare un modello le cui caratteristiche essenziali possono circolare e trovare, previ adattamenti, applicazione universale nelle diverse famiglie giuridiche: in primo luogo, il riferimento ai minori di età — laddove presente — si limita a indicazioni di principio che sollevano la questione relativa alla protezione dei relativi diritti. Emerge come elemento comune una effettiva difficoltà per i legislatori a tradurre in norme operative la tensione tra circostanze di fatto, ovvero la facilità di accesso da parte di minori di età ai servizi e prodotti della società dell'informazione, che porta addirittura nei paesi tecnologicamente avanzati a raggiungere un terzo degli utenti, e meccanismi di protezione di questi

ultimi propri del diritto privato: l'istituto dell'incapacità di agire richiede di essere rivisitato rispetto al paradigma tradizionale legato esclusivamente al compimento del diciottesimo anno di età ⁽²¹¹⁾. Essendo quest'ultimo, infatti, ancorato ad elemento oggettivo, ma puramente di forma volto a tutelare non solo l'infanzia e l'adolescenza in termini di orientare ogni iniziativa al perseguimento dei relativi interessi superiori come criterio prioritario, ma soprattutto a proteggere nelle relazioni contrattuali la sfera patrimoniale dell'incapace. Il sistema, abbiamo osservato, strida a fronte delle esigenze della società dell'informazione che impattano più sulla sfera personale dell'utente, di cui occorre sì preservare sicurezza, incolumità e salute, ma soprattutto consentire di cogliere le opportunità di crescita per costruire la propria personalità e il proprio ruolo da cittadino: la tutela, pertanto, deve potersi coniugare con la costruzione di basi solide per una cittadinanza digitale a partire dallo sviluppo di competenze e conoscenze che siano effettivamente abilitanti a realizzare la propria persona in un ambiente digitale che sia sicuro e alla portata dei giovani utenti.

Si percepisce, dunque nelle legislazioni analizzate, la necessità di regolamentare, da un lato, le basi giuridiche per il trattamento dei dati dei minori di età, specificando l'operatività del meccanismo della rappresentanza legale per prestare il consenso per conto dell'incapace, in ragione della limitata maturità, affinché possa essere messo nelle condizioni di utilizzare le soluzioni digitali e tecnologiche consapevolmente; dall'altro lato, appare altrettanto condivisibile la spinta di alcuni sistemi verso un approccio normativo che, seppur in termini di eccezioni o, in ogni caso, previ gli opportuni bilanciamenti, consenta anche (e almeno) agli adolescenti di poter esercitare maggiori spazi di autonomia. La possibilità di elaborare meccanismi di operatività di forme di autonomia progressiva nella dimensione digitale appare dover essere accompagnata da un duplice fattore: in primo luogo, dall'esigenza che le istituzioni si impegnino ad erogare percorsi formativi, che rafforzino

⁽²¹¹⁾ In dottrina si teorizza un ripensamento dell'incapacità negoziale del minore in favore di una "autonomia progressiva del minore di età" basata sull'interpretazione della CRC e, in particolare, del principio dell'interesse superiore del fanciullo come fonte normativa di rango superiore rispetto a quella primaria, con la conseguenza di dover interpretare il concetto di capacità di discernimento, da accertarsi nel caso concreto e secondo gli usi sociali, come prevalente rispetto al dato formale del compimento del diciottesimo anno di età, così V. BARBA, *Autonomia progressiva e miglior interesse della persona minore di età*, cit.

competenze e conoscenze digitali e rendano edotti gli utenti (minorenni e adulti di riferimento) dei pericoli propri della società dell'informazione e delle misure per prevenirli. In secondo luogo, occorre che meccanismi di verifica dell'età dell'utente consentano di abilitare un regime specifico ai flussi informativi: il che significa identificare un paradigma “*a misura di bambino*”, ove — ad esempio — le informazioni sul trattamento saranno rese con linguaggio semplice e comprensibile e saranno attivati controlli parentali specifici, ovvero sarà attuato *tout court* lo statuto giuridico dei dati sensibili.

Questa interpretazione che emerge dall'osservazione della realtà, oltre il lampione ⁽²¹²⁾, permetterebbe di coniugare il dato formale e oggettivo del compimento di una certa soglia di età con lo sviluppo di competenze specifiche, da valutare caso per caso. Il raggiungimento di certi livelli di maturità e capacità di discernimento, infatti, è fattore meritevole di tutela in termini di acquisizione di spazi di autonomia che sono funzionali al raggiungimento dell'interesse superiore del fanciullo, consentendo di poter realizzare — come vedremo — i propri diritti fondamentali sfruttando le opportunità offerte dalla dimensione digitale, purché ciò avvenga in maniera equa, trasparente e sicura.

Condizione necessaria ad abilitare una maggiore autonomia dell'utente minorenne nella dimensione digitale appare costituita dalla acquisizione, non solo di competenze tecniche, ma soprattutto della capacità di valutare rischi specifici e di sviluppare abilità percettive volte a prevenirli nel caso concreto. Questi ultimi elementi consentono di disegnare i confini della capacità di discernimento, stratificandola in misura inversamente proporzionale alla responsabilizzazione degli operatori economici.

In uno scenario ideale, pertanto, l'utente adolescente che abbia

⁽²¹²⁾ La metafora dell'economista Fitoussi che invitava a cercare “la chiave” oltre la zona illuminata dal lampione (così J.P. FITOUSSI, *Le théorème du lampadaire*, Babel, 2013) è efficacemente ripresa da E. GRANDE, *Lontano dalla luce del lampione: un inedito appunto di viaggio di Rodolfo Sacco*, nel ricordare come il professor Sacco “*mosso dal desiderio di illuminare i luoghi bui del diritto per svelarlo nella sua interezza e complessità, Rodolfo Sacco non può certo fermarsi all'analisi della tradizione giuridica occidentale (...) consegnando alla comparazione l'importantissimo compito di illuminare le zone d'ombra del diritto ovunque*”, in AA.VV., L. ANTONIOLLI, F. CORTESI, E. IORIATTI, B. MARCHETTI (a cura di), *Trento e la comparazione giuridica: voci, esperienze, riflessioni: dalla testimonianza di Rodolfo Sacco e Mauro Cappelletti*, 2024, Edizione Scientifica, p. 99 ss. Si veda, altresì, H. MUIR-WATT, *La fonction subversive du droit comparé*, in *Revue internationale de droit comparé*. Vol. 52 N°3, Juillet septembre 2000, p. 503 ss.

beneficiario di una formazione specifica (da parte delle istituzioni) e di una informazione trasparente e comprensibile (da parte degli operatori) potrebbe essere in grado di discernere in maniera sufficientemente efficace da poter proteggere i propri interessi e diritti in maniera autonoma dai propri genitori, dando prova di saper identificare i possibili pericoli e utilizzare gli strumenti messi a disposizione *by design* e *by default* sia in ottica di prevenzione, che di gestione in caso di diretta esposizione ai rischi. Questo scenario presuppone, pertanto, un livello di consapevolezza e alfabetizzazione e formazione digitale armonizzato e, a fini di *accountability*, quanto meno documentato se non addirittura, come vedremo, certificato. Il che pone ulteriori interrogativi rispetto alle categorie giuridiche coinvolte nella disamina: in primo luogo, abbiamo visto, la tutela della dignità della persona minore di età richiede degli adattamenti rispetto al principio di acquisizione della capacità di agire ⁽²¹³⁾ al compimento della maggiore età, specialmente in un paradigma contrattuale che si allontana dal modello proprietario e possessorio, avvalendosi quotidianamente di meccanismi di accesso a servizi e prodotti.

Le ricadute di sistema possono esaurirsi nella attività di conformità a obblighi di *due diligence* e valutazione, lasciati di fatto all'autoregolamentazione dei servizi della società dell'informazione, oppure occorre ripensare alle categorie giusprivatistiche alla luce di una rinnovata "interpretazione ermeneutica" ⁽²¹⁴⁾ della dignità declinata rispetto alla protezione e promozione dei diritti del minore di età?

⁽²¹³⁾ Recenti studi in materia di capacità di agire mostrano le tensioni di sistema soprattutto con riferimento ai minori di età, L. GIUSTOZZI, *Atti giuridici e capacità di agire*, Edizioni Scientifiche Italiane, 2021, V. BARBA, *Autonomia progressiva e miglior interesse della persona minore di età*, cit., ma la problematica abbraccia anche il tema di coloro formalmente non incapaci di agire, ma particolarmente vulnerabili a fronte dei rischi dei servizi e prodotti della società dell'informazione, specialmente laddove non possa considerarsi assorbita una cultura digitale rispetto ai rischi e alle implicazioni emergenti dal mutamento di paradigma, tradizionalmente legato alla protezione del patrimonio, su modello proprietario e possessorio, verso un sistema di scambi contrattuali fortemente orientati al fornire accesso a flussi di dati. Sul carattere fluido della vulnerabilità digitale, si veda G. MALGIERI, *Vulnerability and Data Protection Law*, cit.

⁽²¹⁴⁾ V. SCALISI, *Ermeneutica della dignità*, cit., p. 106 che richiama la necessità di costruire "dal basso sempre nuovi corrispondenti diritti e doveri finalizzati al pieno e integrale sviluppo della persona umana in un tempo dato e in uno spazio definito, in modo da realizzare un canale di comunicazione diretta e permanente tra il diritto e la vita concretamente vissuta, onde evitare che si determinino fratture o iatus incolmabili, come tali insostenibili da ogni umana convivenza" come risposta allo sviluppo tecnologico che pervade in maniera anche non controllata l'attuale società. Sul punto si veda il

La provocazione richiama il bisogno che la datificazione della società sia regolamentata in maniera armonica rispetto agli strumenti e agli interventi di protezione e promozione propri del diritto dei minori di età espressi nella normativa di settore e, in particolare, rispetto ai contenuti di cui si riempie la formula degli interessi superiori dei bambini.

Occorre a questo punto, dunque, andare ad approfondire le tecniche e le procedure sviluppate per svolgere le attività di valutazione dei rischi, i relativi indici e le necessarie procedure per l'elaborazione e applicazione di *standard* al fine di comprendere quali siano le misure di salvaguardia adottate e adottabili per far fronte ai rischi noti (e quali per quelli non noti), affinché il modello che ci proponiamo di disegnare per una società dell'informazione e una innovazione tecnologica a portata di bambini e adolescenti possa trovare non solo legittimazione sistematica, ma anche efficace attuazione.

commento alla luce del principio personalista di F.D. BUSNELLI, *Le alternanti sorti del principio di dignità della persona umana*, cit.

CAPITOLO II

PROTEGGERE I DIRITTI FONDAMENTALI DEI BAMBINI NELLA DIMENSIONE DIGITALE: LE MISURE TECNICO-ORGANIZZATIVE PER LA MITIGAZIONE DEI RISCHI

SOMMARIO: 1. I diritti fondamentali del fanciullo: la dimensione della CRC. — 1.1. (*Segue*). i rischi nella dimensione digitale e le responsabilità multilivello. — 2. Il sistema di tutele sui prodotti: il precedente delle direttive CE sulla sicurezza dei giocattoli e la nuova direttiva UE sui prodotti difettosi. — 3. Gli approcci nazionali e le implicazioni di sistema. — 3.1. Le misure volte a proibire l'accesso ai minori a determinati servizi: il dibattito negli USA e in Australia. — 3.2. Le misure a portata dei bambini dell'*Online Safety Act*: il pragmatismo britannico. — 3.3. La riforma cinese e l'autonomia c.d. limitata. — 4. La protezione dei fanciulli *by design* e il ruolo degli *standard* tecnici. — 5. La valutazione di impatto con le lenti dei diritti dell'infanzia e il problema tecnico della verifica dell'età. — 6. Sviluppare un sistema di tutele nell'ordinamento italiano a partire dalle esperienze straniere — 6.1. (*Segue*). Le responsabilità genitoriali nella dimensione digitale. — 6.2. (*Segue*). Verso un patentino per l'utente minorenne? — 7. Dalla protezione alla promozione dei diritti fondamentali nella dimensione digitale (*cenni e rinvio*).

Nel capitolo precedente abbiamo ricostruito il quadro giuridico di riferimento per i servizi e i prodotti della società dell'informazione e dell'innovazione tecnologica a partire da un'analisi comparatistica degli approcci legislativi adottati di recente in diversi ordinamenti giuridici.

Abbiamo identificato i principi informatori della materia comuni a più sistemi e osservato, laddove presenti, i meccanismi di tutela rivolti ai minori di età, come categoria di soggetti vulnerabili. In particolare, abbiamo evidenziato la tendenza da parte dei legislatori ad introdurre il consenso del genitore (o del legale rappresentante) come base giuridica dei trattamenti di dati personali concernenti i figli, con una (talvolta) esplicita equiparazione al regime giuridico dei dati sensibili, con conseguente applicazione delle relative misure di salvaguardia. In particolare, abbiamo individuato i bilanciamenti proposti in alcuni

ordinamenti per risolvere la tensione emergente dalla natura progressiva dell'autonomia del minore di età nel crescente sviluppo di capacità di discernimento e abilità ad utilizzare soluzioni digitali e il dato certo e formale della acquisizione della capacità di agire al compimento del diciottesimo anno di età, declinando i possibili scenari applicativi in ottica di perseguimento degli interessi superiori del fanciullo a fronte della pluralità di sollecitazioni che la società dei dati offre, soprattutto agli adolescenti.

In questo capitolo, pertanto, esploreremo i diritti fondamentali dei bambini, così come internazionalmente riconosciuti nella Convenzione ONU sui diritti dell'infanzia e dell'adolescenza (di seguito, anche in questo capitolo, "CRC"), per declinarli nella dimensione digitale al fine di comprendere in maniera più specifica in cosa consistano le esigenze di protezione e come si articolino le vulnerabilità per l'uso degli strumenti tecnologici e dei servizi digitali da parte dei minori di età. L'analisi è volta a delineare — nell'ambito degli elementi comuni alla cornice che segna i confini del paradigma comune del sistema di tutele dei diritti dei minori nella dimensione digitale — l'impatto delle misure tecniche e organizzative implementate in osservanza degli obblighi di valutazione dei rischi per i minori di età, imposti dalle normative di settore, rispetto alla mitigazione delle vulnerabilità e alla promozione del principio del c.d. *best interest of the child* ⁽¹⁾.

In particolare, metteremo a sistema il ruolo dell'alfabetizzazione rispetto ai sistemi di IA e dell'educazione digitale con i paradigmi di responsabilizzazione e di responsabilità rispetto ai diritti fondamentali dei bambini nella dimensione digitale, con l'obiettivo di valorizzare forme di autonomia del giovane utente, proponendo meccanismi di tutele a geometria variabile, suscettibili di poter essere attuati — con i dovuti adattamenti — in diversi ordinamenti.

(1) N. HELBERGER, M. SAX, J. STRYCHARZ, H.-W. MICKLITZ, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, cit., C. RIEFA, *Protecting vulnerable consumers in the digital single market*, in *European Business Law Review*, 2022, 33, 607. Sulle vulnerabilità digitali e digitalizzazione delle vulnerabilità sia concesso rinviare a D. AMRAM, *La transizione digitale delle vulnerabilità e il sistema delle responsabilità*, in *Riv. it. med. leg.*, 2023, p. 1 ss.

1. I diritti fondamentali del fanciullo: la dimensione digitale della CRC.

La CRC fonda la tutela e la promozione dei minori di età attraverso l'obbligo degli Stati firmatari di adottare provvedimenti volti a proteggere il loro interesse superiore in qualsiasi contesto che li coinvolga, incluso oggi — pertanto — l'ambiente digitale e il rapporto con le nuove tecnologie. Ciò significa, da un lato, interpretare i diritti enunciati per garantire il benessere dei fanciulli nella dimensione reale, caratterizzata da rapporti e interazioni interpersonali, affinché siano altrettanto rappresentativi degli interessi meritevoli di tutela nella società dell'informazione e, dall'altro, verificare l'efficacia dei sistemi di tutela esistenti per promuovere le opportunità di crescita offerte dalle tecnologie, senza esporre i giovani utenti a possibili pregiudizi.

A questo riguardo, il principio generale del divieto di discriminazione previsto dall'art. 2 CRC e quello dell'interesse superiore del bambino, enunciato al successivo art. 3 CRC, richiedono agli Stati firmatari di introdurre meccanismi di attuazione specifici per la dimensione digitale. Infatti, la sfida attuale è quella di comprendere di quali nuovi contenuti le due formule astratte possano riempirsi, considerate le caratteristiche dello spazio digitale e delle applicazioni tecnologiche. Occorre, infatti, un adattamento rispetto ai consueti parametri che nella realtà fisica rendono possibile il bilanciamento tra diritti e interessi nell'interpretazione *ex casu*. A questo proposito, vedremo come la scelta di *standard* tecnici piuttosto che di misure organizzative possa contribuire a definire regole di diligenza appropriate in ragione delle caratteristiche (e delle vulnerabilità) di cui ciascun bambino è portatore ⁽²⁾.

L'art. 4 CRC *a priori* richiede agli Stati Membri l'impegno, anche in termini di risorse, affinché gli interventi necessari ad attuare i diritti di natura patrimoniale, sociale e culturale siano implementati, anche attraverso meccanismi di cooperazione internazionale. L'art. 5 CRC giustifica il coinvolgimento, oltre che di genitori e di legali rappresentanti, anche di adulti di riferimento o comunità locali. Non è un caso che le successive disposizioni siano dedicate all'enunciazione dei diritti rispettivamente alla vita, identità e famiglia (artt. 6-11 CRC), alla libertà di espressione, opinione, di pensiero e credo religioso (artt. 12-14 CRC)

(2) A. MANSFERRER, E. GARCIA-SÁNCHEZ (a cura di), *Human Dignity of the Vulnerable in the Age of Rights*, Dordrecht: Springer, 2016.

e alla libertà di associazione in pace (art. 15 CRC): nessuno di questi appare trovare barriere ad una promozione *tout court* nella dimensione digitale. Per tale ragione, pare potersi confermare che, laddove si consideri l'elenco sufficientemente esaustivo per promuovere la crescita del minore in armonia con i valori condivisi dalla comunità internazionale delle Nazioni Unite per la dimensione fisica, lo stesso valga per quella digitale ⁽³⁾.

Il diritto del fanciullo di esprimere la propria opinione e di essere ascoltato costituisce — peraltro — fondamento giuridico per la definizione di sempre più crescenti spazi di autonomia (anche negoziale) per il minore di età che, in particolare, si manifestano nella dimensione digitale laddove agiscono come utenti di servizi a loro direttamente destinati. Tuttavia, nelle attività *online*, o supportate da nuove tecnologie, si assiste ad una maggiore esposizione a possibili arbitrarie e illecite interferenze nella vita privata, familiare, domestica e alla corrispondenza privata da parte di terzi, nonché a possibili attacchi all'onore e reputazione del bambino che si manifestano anche in fenomeni noti come *cyberbullismo* ⁽⁴⁾, non prevedibili o gestibili a causa della possibile immaturità emotiva, psicologica del bambino, quale soggetto in formazione ⁽⁵⁾, rispetto all'utente adulto. Questi profili trovano, dunque, tutela generale nell'ambito dell'art. 16 CRC, laddove si richiedono specifiche misure di salvaguardia, anche di tipo tecnologico, da implementare in ogni applicativo al fine di costruire un robusto sistema di prevenzione e mitigazione dei rischi di pregiudizio, senza necessità di ulteriori specificazioni. Prende forma, in questo contesto, infatti, un intervento di responsabilizzazione degli operatori della società dell'informazione che si accompagna a quello dei legali rappresentanti e degli adulti di riferimento volto a promuovere azioni educative destinate a preservare l'esposizione del singolo, ma anche della comunità di riferimento, rispetto a qualsivoglia (illecita) ingerenza nella sfera della riservatezza della persona, anche minore di età.

Ancora, proseguendo nell'analisi della Convenzione, l'art. 17

⁽³⁾ J. TOBIN, *The UN Convention on the Rights of the Child: A Commentary*, Oxford Commentaries on International Law, 2019, M.R. SAULLE, *Codice internazionale dei diritti del minore*, ESI, Napoli, 1992.

⁽⁴⁾ J. TOBIN, *op. ult. cit.*

⁽⁵⁾ E. BATTELLI (a cura di), *Diritto privato delle persone minori di età*, cit. Nell'ambito del medesimo volume, si veda anche il contributo di F. RUGGIERI, *Minori e privacy*, p. 139 ss.

CRC ⁽⁶⁾ appare particolarmente attuale sebbene rivolto ai *mass media* nell'accezione ben lontana da quella che si intende oggi per mezzi di comunicazione nella società dell'informazione. A rendere attuale la disposizione si pone la lungimiranza con cui è costruita. La norma coglie il potenziale offerto da tali strumenti rispetto alla formazione culturale della personalità del bambino in termini di inclusione e valorizzazione delle diversità, sia in quanto si menzionano una serie di sfide senza tempo, come il raggiungimento del benessere sociale, spirituale e morale, sia perché si riferisce alla tutela della salute mentale e fisica. Si tratta di fattori di notevole rilevanza al fine di indirizzare quelle valutazioni di impatto oggi richieste dalle normative sulla digitalizzazione della società.

L'invito dell'art. 17 CRC alla parità di accesso ai mezzi di comunicazione di massa e ai relativi contenuti è, infatti, rivolto agli Stati firmatari, ma anche (e soprattutto) agli operatori di settore, affinché la diffusione di informazioni e materiale sia tesa a sviluppare e potenziare le personalità, i talenti, e le abilità fisiche e psichiche dei bambini. Si raccomanda, inoltre, l'utilizzo di una varietà di fonti, a misura di bambini, incoraggiando le minoranze linguistiche a fini di maggiore inclusività nell'accesso alle risorse multimediali. L'adozione di linee guida volte a rendere consapevoli i bambini stessi dei loro diritti e delle potenzialità è, infine, incoraggiata dalla stessa disposizione ⁽⁷⁾. Queste indicazioni ben si prestano ad essere adattate alle funzionalità oggi offerte dalle piattaforme digitali e dalle tecnologie, soprattutto laddove lette in combinato disposto con l'art. 19 CRC. Quest'ultima norma, infatti, impone agli Stati firmatari, in particolare, di implementare misure legislative, amministrative, sociali ed educative per prevenire ogni forma di violenza fisica o psicologica, danno o abuso, trascuratezza o maltrattamento, incluso lo sfruttamento e l'abuso sessuale. In questa prospettiva, si riproduce il paradigma di tutela multilivello guidato, da un lato, dalle opportunità da cogliere e promuovere e, dall'altro, dai rischi da valutare e mitigare.

⁽⁶⁾ G. LANSDOWN, (2022). *Article 17: The Right to Access to Diverse Sources of Information*. In: VAGHRI, Z., ZERMATTEN, J., LANSDOWN, G., RUGGIERO, R. (eds), *Monitoring State Compliance with the UN Convention on the Rights of the Child. Children's Well-Being: Indicators and Research*, vol 25. Springer, Cham. https://doi.org/10.1007/978-3-030-84647-3_12.

⁽⁷⁾ Si richiama l'art. 29 CRC.

1.1. (Segue). *I rischi nella dimensione digitale e le responsabilità multilivello.*

La transizione digitale di servizi e prodotti impatta sull'attuazione dei diritti illustrati nel precedente paragrafo, in quanto nello spazio virtuale le esposizioni alla relativa compromissione sono più frequenti in termini di occorrenza, ovvero più gravi per la possibile serietà del pericolo, con il conseguente incremento del rischio per utenti-bambini di possibili pregiudizi, con implicazioni di diversa gravità per il relativo sviluppo psicofisico. Come nel caso sopra-menzionato del *cyberbullismo*, è la sfera della riservatezza, dell'onore e della reputazione della vittima ad essere compromessa, provocando talvolta disagi e ansie, talaltra inducendo condotte addirittura autolesive, con possibili danni permanenti all'equilibrio psicologico e anche fisico del bambino. Il dato statistico sul punto è allarmante: non solo sussiste una correlazione tra la crescita dei suicidi per *cyberbullismo* e il tempo trascorso dal minore *online*, ma la stessa assume carattere esponenziale ⁽⁸⁾.

Ulteriori problematiche, invece, emergono da ipotesi di sfruttamento e abusi della condizione di incapacità di discernimento dei minori di età. Fenomeni come il *grooming*, il *sexting*, ma anche le manipolazioni di contenuti a rilevanza sessuale o pornografica, sia ad opera di minori stessi, che di soggetti maggiorenni, portano a conseguenze devastanti sulla crescita e libertà della vittima ⁽⁹⁾.

A tal proposito, occorre rilevare che la semplice introduzione di

⁽⁸⁾ Un recente studio negli USA riferisce che quasi il 15% dei minori è vittima di episodi di cyberbullismo e oltre il 13% si espone a tentativi di suicidio, così A. SCHONFELD, D. McNIEL, T. TOYOSHIMA, R. BINDER, *Cyberbullying and Adolescent Suicide*. J Am Acad Psychiatry Law. 2023 Mar; 51(1):112-119. doi: 10.29158/JAAPL.220078-22. Epub 2023 Feb 23. PMID: 36822834. Sulla correlazione tra suicidi negli adolescenti e utilizzo di strumenti digitali, si veda D.S. MANTEY, R.A. YOCKEY, A.E. SPRINGER, *Digital screen time and suicidality during high school: How important is cyberbullying? A mediation analysis using the youth risk behavioral surveillance survey, 2011-2019*. Prev. Med. 2023 Jan; 166:107330. doi: 10.1016/j.ypmed.2022.107330. Epub 2022 Nov 9. PMID: 36334685.

⁽⁹⁾ Si pensi alla tecnologia DeepFake utilizzata da App capaci di elaborare immagini di donne e restituirle nude, chiamate DeepNude, o BikiniOff, su cui l'Autorità Garante italiana ha aperto un'istruttoria, qui disponibile: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9470722>. Un recente studio spagnolo supporta una proposta di legge volta a vietare l'uso dei *social network* ai minori di sedici anni di età, Comité de expertos para la creación de entornos digitales seguros para la infancia y la juventud, *Informe del comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud e infancia*, 2024,

sistemi di controllo e monitoraggio dell'uso delle tecnologie non sembra sufficiente a prevenire l'esposizione a questi pericoli. I principi enunciati richiedono l'introduzione di misure sempre più sofisticate volte ad anticipare — in ottica di prevenzione — possibili vulnerabilità, non solo a fronte di un uso improprio degli strumenti informativi, ma anche in caso di utilizzo secondo i termini e condizioni stabiliti, che possa — tuttavia — essere foriero di accessi non autorizzati, o manipolazioni, o condotte in ogni caso non lecite: per questo motivo non è sufficiente richiedere ai prestatori di servizi digitali di moderare i contenuti, ma occorre, altresì, che siano presenti strumenti capaci di far segnalare pericoli e richiedere interventi in presa diretta dagli utenti stessi.

A questo proposito, la Convenzione di Lanzarote approvata dal Consiglio d'Europa coniuga meccanismi di responsabilità e di responsabilizzazione laddove stabilisce, da un lato, all'art. 6, un dovere di educare i minori affinché siano consapevoli delle possibili situazioni di rischio rispetto al pericolo di sfruttamento e abusi sessuali — specialmente nella dimensione tecnologica e digitale — affinché acquisiscano contezza delle misure di protezione sulla base delle relative capacità cognitive; dall'altro lato, agli articoli 8 e 9, responsabilizza la società, affinché promuova sia nel settore pubblico, che in quello privato, azioni di sensibilizzazione e di prevenzione e segnalazione in materia ⁽¹⁰⁾.

Vedremo in seguito come queste disposizioni contribuiscano allo sviluppo delle valutazioni di impatto, che gli operatori sono chiamati ad effettuare alla luce della normativa dell'UE sui servizi digitali e sull'intelligenza artificiale ⁽¹¹⁾.

Dagli esempi riportati, appare evidente che la dimensione digitale costituisca uno scenario alternativo a quello fisico, ove i minori di età possono realizzare la propria persona, incontrando — pertanto — rischi comuni e propri, da mitigare *by design* e *by default*, al fine di non subire conseguenze dannose. Allo stesso tempo, tuttavia, per una efficace promozione dei diritti dei minori nella dimensione digitale, occorre ricostruire, proprio dalle carte internazionali un paradigma

disponibile qui: <https://www.juventudeinfancia.gob.es/es/infancia/comit%C3%A9-expertos-creaci%C3%B3n-entornos-digitales-seguros>.

⁽¹⁰⁾ Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e gli abusi sessuali, 25 ottobre 2007, disponibile <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=201>.

⁽¹¹⁾ *Infra* §§4 e 5.

multilivello di ruoli e responsabilità da distribuire tra istituzioni, scuole, famiglie e genitori, e tutta la comunità di riferimento per il minore affinché ciascuno si adoperi perché l'ambiente digitale frequentato possa essere alla portata del singolo bambino.

Su questa scia, si inserisce la Carta dei diritti fondamentali dell'Unione Europea ⁽¹²⁾, che dedica alcuni articoli del Capo IV sull'uguaglianza, alle categorie di soggetti più deboli: minori di età (art. 24), anziani (art. 25), disabili (art. 26) ⁽¹³⁾.

In particolare, l'art. 24 enuncia il diritto "*alla protezione e alle cure necessarie per il loro benessere*", individuando speculari responsabilità, da un lato, in capo ad autorità pubbliche e private (citato al secondo comma), affinché assicurino tale tutela e al contempo perseguano gli interessi superiori del fanciullo in ogni atto e, dall'altro lato, in capo ai genitori, destinatari del terzo comma, nell'ambito del diritto alla bigenitorialità. La norma riconosce altresì la libertà del minore di età di esprimere la propria opinione e di essere ascoltato sulle questioni che lo interessano, tenendo conto dell'età anagrafica e delle maturità psicofisica.

Come ricordato nel capitolo precedente, l'art. 24 della Carta dei diritti fondamentali costituisce il perno del sistema di tutele per i minori di età intorno al quale, sia il legislatore dell'UE, che quelli dei singoli Stati Membri devono costruire le strategie di attuazione dei diritti fondamentali del fanciullo nelle normative di settore.

Alla luce dell'art. 24, pertanto, l'esercizio delle responsabilità genitoriali nella dimensione digitale assume una duplice connotazione. Rispetto ai rischi noti, propriamente digitali ovvero comuni alla dimensione fisica, come quelli evidenziati nel paragrafo precedente, il ruolo del genitore è quello di fornire gli strumenti per proteggere il figlio anche attraverso una educazione digitale adeguata all'età e all'esposizione (ovvero all'uso quotidiano). L'approccio non si discosta da qualsiasi altra attività che coinvolga il minore di età, se non per i contenuti specifici degli interventi educativi.

Rispetto ai rischi non noti, invece, la cura per il minore si declina in termini di responsabilizzazione secondo un paradigma più ampio che coinvolge non solo i genitori, ma gli operatori di settore, le

⁽¹²⁾ Carta dei diritti fondamentali dell'UE, Nizza, 2000, https://www.europarl.europa.eu/charter/pdf/text_it.pdf.

⁽¹³⁾ AA.VV., M.G. ZECCA (a cura di), *Le famiglie nello spazio europeo*, Milano, 2023.

istituzioni e più in generale la società attraverso una distribuzione di ruoli emergenti dal quadro regolatorio in materia di strategia digitale e innovazione. Al pari di un titolare di trattamento nella propria organizzazione, il genitore sarà responsabile di effettuare una valutazione caso per caso per ciascuno scenario e per ciascun figlio al fine di decidere quali misure introdurre nella quotidianità al fine di proteggere e promuovere i diritti dei propri figli.

Rientrano in questo approccio sia gli interventi formativi ed educativi per rendere più consapevole il minore non solo dei rischi, ma anche delle potenzialità dei servizi della società dell'informazione, sia l'introduzione di misure di sicurezza per il controllo e monitoraggio dei sistemi a disposizione dei minori al fine di verificarne o, addirittura limitarne — *by design* — l'accesso ad ambienti sicuri ovvero l'uso a determinate condizioni. Anche in questo caso, premesso un certo grado di conoscenza da parte del genitore, la strategia educativa non appare metodologicamente diversa da quella volta a proteggere la prole in qualsiasi ambiente considerato pericoloso. Si pensi allo scenario dell'ingresso in una piscina: fino ad una certa età (in genere 14 anni) il gestore della struttura esclude l'ingresso a minori non accompagnati, si promuovono corsi di nuoto per tutte le età, esistono strutture dotate di piscine con altezze diversificate. Tutto ciò premesso, ci sarà il genitore che — in ragione dell'età o dell'altezza della piscina o del numero e tipologia di utenti — starà in acqua col figlio, a bordo piscina o all'ombrellone, articolando con misure ritenute appropriate la propria condotta per meglio ottemperare al proprio obbligo di vigilanza. Allo stesso modo, l'accompagnamento del genitore diventa progressivamente meno necessario in ragione di una crescente autonomia del singolo valutata dall'esercente le responsabilità genitoriali per autorizzare l'accesso (o banalmente finanziarlo) e il gestore della piscina nelle more della fruizione del servizio.

La difficoltà di tradurre lo scenario della piscina ai nostri fini di indagine consiste nella mancata circoscrizione, nella specie, dei tempi (la struttura prevede orari di apertura e di chiusura definiti) e dello spazio degli interventi, in quanto l'ambiente digitale è, di fatto, sempre accessibile.

Il ruolo di responsabilizzazione del genitore può, tuttavia, essere supportato da elementi tecnici attraverso l'introduzione di filtri spaziotemporali in modo da limitare l'esposizione ad ambienti verificati per

un numero massimo di ore consecutive/giornaliere e di bloccare l'esposizione a contenuti riservati a un pubblico maggiorenne ⁽¹⁴⁾.

Conseguentemente, l'attivazione dei sistemi di controllo genitoriale di base resi disponibili sui dispositivi appare una misura di salvaguardia minima che il genitore può introdurre per esercitare diligentemente le proprie responsabilità. D'altro canto, tali strumenti non saranno sufficienti, se non accompagnati da interventi educativi appropriati per lo specifico utente-bambino e da un monitoraggio effettivo dell'utilizzo dei servizi della dimensione digitale, con un bilanciamento progressivamente sempre più orientato a rendere autonomo l'utente in ragione della dimostrata capacità di prevenire (e gestire qualora occorramo) i menzionati rischi.

2. Il sistema di tutele sui prodotti: il precedente delle direttive CE sulla sicurezza dei giocattoli e la nuova direttiva UE sui prodotti difettosi.

L'esposizione dei minori di età a pericoli nelle attività quotidiane non è senz'altro una condizione nuova. Al livello comunitario, già nel 1988, era stata adottata una direttiva in materia di sicurezza dei giocattoli ⁽¹⁵⁾, volta a stabilire “*i requisiti essenziali (...) compresi i requisiti specifici di sicurezza in materia di proprietà fisiche e meccaniche, infiammabilità, proprietà chimiche, proprietà elettriche, igiene e radioattività*”, rivista e aggiornata alla luce dell'impatto dello sviluppo tecnologico nel settore nel 2009 ⁽¹⁶⁾, al fine di meglio proteggere sicurezza e salute dei consumatori.

La tecnica legislativa adottata prevede l'introduzione di una meto-

⁽¹⁴⁾ Si veda a tal proposito la delibera AGCM, *Adozione delle linee guida finalizzate all'attuazione dell'articolo 7-bis del decreto-legge 30 aprile 2020, n. 28 in materia di “sistemi di protezione dei minori dai rischi del cyberspazio”*, che stabiliscono, ad esempio, la pre-attivazione gratuita dei *parental control* per i contratti di fornitura nei servizi di comunicazione elettronica da applicarsi in caso di offerte riservate a un pubblico di minorenni (o altrimenti su richiesta) e consistenti in meccanismi di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore agli anni diciotto.

⁽¹⁵⁾ La direttiva 88/378/CEE del Consiglio, del 3 maggio 1988, relativa al ravvicinamento delle legislazioni degli Stati membri concernenti la sicurezza dei giocattoli.

⁽¹⁶⁾ Direttiva UE del 18 giugno 2009, n. 48, sulla sicurezza dei giocattoli <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32009L0048>.

dologia di analisi e mitigazione del rischio attraverso l'introduzione di obblighi per gli operatori economici (fabbricanti, importatori e distributori) al fine di responsabilizzare la messa sul mercato e libera circolazione di prodotti non solo conformi agli *standard* di sicurezza richiesti per la marcatura CE ⁽¹⁷⁾, ma anche tenendo conto della vulnerabilità del consumatore minore di età che potrebbe utilizzare il prodotto anche in maniera impropria. In quest'ottica la direttiva raccomanda di tenere un approccio di protezione *by design* e *by default*, considerando gli usi prevedibili “*del bambino, solitamente sprovvisto del tasso di diligenza media proprio dell'utilizzatore adulto*”, invitando a progettare misure di salvaguardia, onde limitare rischi in caso di uso improprio da parte dell'utente minore di età, ovvero disciplinando “*il rischio residuo attraverso informazioni relative al prodotto destinate a chi effettua la supervisione, tenendo conto della loro capacità di affrontare*” lo stesso, anche integrando le avvertenze.

Gli articoli 10 e 11 della direttiva, dunque, introducono requisiti essenziali di sicurezza e meccanismi di monitoraggio e controllo e relativa conservazione a fini di esibizione in caso di attività di vigilanza da parte dell'autorità competente, mentre l'art. 18 della valutazione di sicurezza rispetto alla potenziale esposizione a “*pericoli chimici, fisico-meccanici ed elettrici, di infiammabilità, di igiene e di radioattività che il giocattolo può presentare*”. Infine, gli allegati, tra le altre, circoscrivono l'ambito di applicazione escludendo alcuni giocattoli e identificano particolari requisiti di sicurezza sulla base delle proprietà fisico-meccaniche o chimiche o elettriche, l'attitudine all'infiammabilità o alla radioattività, o all'igiene.

Anche nell'evoluzione della regolamentazione dei servizi audiovisivi, come osservato nel capitolo precedente, si coglie l'esigenza di adeguare le misure di protezione allo sviluppo di funzionalità tecnologicamente più avanzate e al relativo uso, andando in una direzione di protezione *by design* e *by default* dei minori, rispetto non solo a pericoli diretti di esposizione a contenuti nocivi, ma si introduce il parametro dell'appropriatezza rispetto alla promozione dei diritti fondamentali del minore, che include il divieto di sfruttamento commerciale dei dati e del comportamento del bambino come consumatore della società dell'informazione. La Direttiva UE n. 2018/1808, infatti, coglie le sfide

(17) La marcatura CE è disciplinata dal Reg. UE 9 luglio 2008, n. 765 in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti.

lanciate dall'impatto che servizi di piattaforma per la condivisione di video hanno sul grande pubblico e, in particolare, sulla giovane utenza, sollecitando l'adozione di misure che evitino l'esposizione dei bambini a comunicazioni commerciali aventi ad oggetto bevande alcoliche o il gioco d'azzardo, o a contenuti che possano nuocere al loro sviluppo fisico, mentale o morale, istigare alla violenza o esporli a discorsi d'odio, specificando che i contenuti più nocivi come *“la violenza gratuita e la pornografia”* debbano essere soggetti a misure più rigorose ⁽¹⁸⁾. Allo stesso modo, come osservato, è vietato lo sfruttamento della *“inesperienza o credulità”* nei messaggi promozionali.

L'introduzione di misure tecniche e organizzative volte a prevenire l'esposizione a contenuti inappropriati da parte dei minori di età passa dall'elaborazione di obblighi informativi dei prestatori di servizi, all'introduzione di contenuti in determinate fasce temporali, al subordinare l'accesso ai contenuti alla verifica dell'età dell'utente ⁽¹⁹⁾.

Un principio rilevante espresso in questo contesto è quello di

⁽¹⁸⁾ Consideranda 45 e 47 e articolo 6-*bis* della Direttiva UE n. 2018/1808, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi (direttiva sui servizi di media audiovisivi), in considerazione dell'evoluzione delle realtà del mercato.

⁽¹⁹⁾ Le misure tecnico-organizzative introdotte per proteggere l'utente minore di età si possono classificare in tre macro-aree, onde evitare l'esposizione a contenuti non appropriati o dannosi: quelle relative all'informazione trasparente (come l'identificazione di fasce di età per le quali il contenuto è appropriato, l'esibizione di etichette di classificazione per anticipare i temi, l'accesso guidato alle proposte), ovvero quelle relative all'identificazione di intervalli di tempo protetti (escludendone la proiezione anche in prossimità delle fasce orarie identificate), ovvero introducendo barriere tecniche come contenuti accessibili previa verifica dell'età o attraverso codici riservati a utenti adulti, da attivarsi su base volontaria. Tali misure — adottate anche attraverso codici di autoregolamentazione — devono essere adattate alla tipologia del servizio (trasmissioni, prodotti a richiesta, piattaforme per la condivisione, etc) e alle realtà di mercato. Si veda ERGA, *Protection of Minors in the Audiovisual Media Services: Trends & Practices*, 2016, disponibile <https://erga-online.eu/wp-content/uploads/2016/10/ERGA-PoM-Report-2017-wordpress.pdf>. In Italia il D.lgs. 8 novembre 2021, n. 208, *Attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato*, ha abrogato il precedente Testo Unico del 2005 che già introduceva — favorendo l'autoregolamentazione — l'introduzione delle menzionate misure.

separazione dei fini tra il trattamento dei dati personali allo scopo di attivare le misure tecniche e organizzative per evitare l'esposizione del minore a contenuti nocivi, considerato non solo lecito, ma altresì doveroso, rispetto all'utilizzo delle medesime informazioni a fini commerciali, di *marketing* diretto o profilazione, che invece sono vietati ⁽²⁰⁾.

Sulla scia dell'esperienza europea in questi due settori (quello dei giocattoli e dei servizi audiovisivi) già da decenni proiettata a richiedere specifiche misure tecniche e organizzative agli operatori economici per mitigare i rischi che prodotti e servizi destinati all'uso prevalente di bambini possono occorrere, si possono leggere le iniziative legislative, anche nazionali, volte ad esplicitare i meccanismi di tutela *by design* e *by default* per i servizi digitali e i sistemi basati sull'intelligenza artificiale.

In questo contesto, si inserisce la recente Direttiva UE n. 2024/2853 sui prodotti difettosi, volta a definire i principi per chiarire i confini della responsabilità del produttore in considerazione della transizione digitale dell'economia. In particolare, per quanto rileva ai nostri fini, la definizione di prodotto alla luce della novella include anche “*file di fabbricazione digitale e software*” e le piattaforme *online* possono essere ritenute responsabili per un prodotto difettoso alla stregua di qualsiasi altro operatore economico. Inoltre, per la determinazione del carattere difettoso di un prodotto, il parametro dell’“*uso ragionevolmente prevedibile*” deve essere interpretato — al pari di quanto osservato per i giocattoli — considerando le attitudini e le vulnerabilità degli utenti, portando l'esempio dei bambini ⁽²¹⁾. Le ricadute applicative potrebbero essere notevoli, considerando che, in sede di recepimento, anche la mancata introduzione di misure che proteggano i minori *online*, come la possibilità di aggirare i meccanismi di verifica dell'età dell'utente, potrebbero soddisfare i requisiti di difettosità del prodotto digitale. Peraltro la direttiva esplicita la risarcibilità sia di pregiudizi patrimoniali che non patrimoniali, di conse-

⁽²⁰⁾ Considerando 21 e art. 6 *bis* della Direttiva UE n. 2018/1808, cit.

⁽²¹⁾ Considerando 31 specifica che l'uso ragionevolmente prevedibile, che può valutare il carattere difettoso del prodotto, comprenda “*anche un abuso che non sia irragionevole in determinate circostanze, come il comportamento prevedibile dell'utilizzatore di una macchina causato dalla mancanza di concentrazione o il comportamento prevedibile di determinati gruppi di utenti, come i bambini*”, Dir. UE 23 ottobre 2024, n. 2853 sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio.

guenza si aprono scenari di possibile distribuzione di responsabilità e legittimazione di azioni risarcitorie che potrebbero colmare alcune pretese non rilevanti per il GDPR o per il DSA ⁽²²⁾: si pensi, ad esempio, al contenzioso che si è sviluppato oltreoceano verso i *chatbot*, ritenuti dai familiari responsabili di aver portato gli utenti a conseguenze estreme ⁽²³⁾.

Ci si può interrogare, dunque, se, considerata la valutazione del rischio di recare pregiudizio specialmente ad utenti vulnerabili, il mancato funzionamento di una misura tecnico-organizzativa di prevenzione, come la mancata verifica dell'età o la falla nell'impedire l'esposizione a determinati contenuti, possa configurare una ipotesi di difettosità, alla luce del prevedibile uso (improprio) che l'utente minorenni potrebbe ragionevolmente farne e così concretizzare il rischio per la salute, incolumità, sicurezza in un pregiudizio.

Vedremo nei prossimi paragrafi quali siano le misure tecniche e organizzative che le legislazioni nazionali hanno più o meno esplicitamente introdotto e la relativa rilevanza nella distribuzione di responsabilità volte a proteggere i minori di età.

3. Gli approcci nazionali e le implicazioni di sistema.

Dalla prospettiva di responsabilizzazione multilivello prendono forma le misure tecnico-organizzative volte a limitare *by default* certi usi e consentire una più efficace attività di controllo e monitoraggio.

In termini di politica del diritto, come abbiamo osservato nel

⁽²²⁾ Mentre l'art. 82 del GDPR prevede un regime specifico per l'azione risarcitoria, al fine di disciplinare i rapporti tra titolare e responsabile del trattamento, l'art. 54 del DSA richiama la normativa dell'UE e nazionale, stabilendo — di fatto — che la violazione degli obblighi imposti dallo stesso regolamento possa dar luogo ad azioni risarcitorie in caso di conseguenti pregiudizi all'utente.

⁽²³⁾ Il dibattito è particolarmente attuale: in Florida un genitore ha depositato un ricorso per accertare la responsabilità dell'applicativo Character AI per l'istigazione al suicidio del proprio figlio. Quest'ultima ha nel frattempo rilasciato un comunicato di aver introdotto delle funzionalità pop-up laddove l'utente inserisca input che sono collegati a forme di autolesionismo o suicidio reindirizzando l'utente al National Suicide Prevention Lifeline, *Community Safe Updates*, <https://blog.character.ai/community-safety-updates/>. In precedenza è stata altresì organizzata una sorta di class action dall'International Association for Suicide Prevention. In maniera provocatoria, si veda l'intervento di G. SCORZA, *Istruzioni per morire dal mio amore artificiale*, L'Espresso, 6 settembre 2024.

precedente capitolo, la pluralità di approcci nazionali converge in ogni caso verso alcune linee di indirizzo che consentono di classificare le misure adottate e commentarne le implicazioni pratiche. Certi sistemi stanno discutendo (o hanno già adottato), ad esempio, l'introduzione di divieti generali di accesso e uso da parte di minori di età, resi relativi dall'implementazione di specifiche salvaguardie tecniche da parte dei genitori o da chi esercita le responsabilità genitoriali. Si tratta, infatti, di meccanismi di validazione dei profili per la registrazione a piattaforme digitali, di monitoraggio per l'uso e limitazione in certe fasce orarie onde evitare fenomeni di dipendenza, giornalieri e, soprattutto, viste le prassi ⁽²⁴⁾, notturni.

Nei paragrafi che seguono esploreremo in maniera più granulare certe iniziative già menzionate nel primo capitolo che, invero, a partire dal quadro normativo sulla datificazione, non si limitano ad indirizzare la vulnerabilità dei minori di età in maniera generica, ma si occupano di fornire strumenti per rendere operativa la tutela dell'utente minorenne rispetto a specifici rischi. In particolare, identificheremo degli elementi comuni o particolarmente efficaci suscettibili di trovare applicazione in una pluralità di ordinamenti e contribuire a disegnare un sistema di tutele e promozione dei diritti dei bambini e degli adolescenti nella dimensione digitale che possa essere suscettibile di circolare e trovare validazione nei principi informativi della materia.

3.1. *Le misure volte a proibire l'accesso ai minori a determinati servizi: il dibattito negli USA e in Australia.*

Nel capitolo precedente abbiamo accennato come la frammentarietà delle iniziative su dati e innovazione tecnologica negli USA costituisca un limite all'identificazione di misure che possano contribuire alla costruzione di un modello armonizzato di gestione responsabile dei servizi e dei prodotti della società dell'informazione.

A tal proposito, appare rilevante illustrare le iniziative di *soft law* che consentono di identificare dei parametri per orientare le interpretazioni più restrittive proposte al livello nazionale. Ad esempio, la Federal Trade Commission ha elaborato alcune linee guida per suppor-

⁽²⁴⁾ NHS ha sviluppato un servizio per la valutazione del grado di dipendenza da videogiochi, <https://www.cnwl.nhs.uk/national-centre-gaming-disorders>.

tare gli operatori a conformarsi al COPPA ⁽²⁵⁾. In particolare, con riferimento alla necessità di verificare l'effettiva prestazione del consenso del genitore al trattamento dei dati personali dei figli minori di tredici anni, le linee guida identificano alcune misure che si rendono suscettibili di applicazione anche in altri contesti. Laddove si specifica, infatti, che sia richiesta la forma scritta, si elencano altresì delle alternative: ovvero l'utilizzo di sistemi di pagamento che trasmettano notifiche al titolare del conto, ovvero di strumenti di verifica asincrona a mezzo di contatto telefonico o in videoconferenza, oppure la trasmissione di documenti di identità e sottoposizione a strumenti di riconoscimento facciale. Le linee guida si occupano altresì di individuare i contenuti minimi dell'informativa sul trattamento di dati per ottemperare agli obblighi di trasparenza, nonché di indicare metodologie per assicurare la sicurezza dei flussi.

Rispetto al versante legato all'esposizione di minori a contenuti nocivi o impropri, oltre alla proposta di estensione delle tutele anche agli adolescenti — con il già illustrato COPPA 2.0, merita una riflessione anche il c.d. Kids Online Safety Act (KOSA) ⁽²⁶⁾, che si rivolge ai prestatori di servizi digitali, affinché adottino meccanismi specifici di prevenzione sin dalla progettazione delle piattaforme rispetto al manifestarsi di disordini mentali, come dipendenze, o di comportamenti violenti e abusi sessuali negli utenti, rivolgendosi sia ai bambini, minori di anni tredici, sia agli adolescenti, minori di diciassette.

In particolare, l'iniziativa andrebbe a incidere sui rischi connessi all'impatto dei servizi digitali sull'adozione di comportamenti nocivi per “*kids*”, in quanto introduce divieti di forme di promozione del mercato di droghe, tabacco o alcol, nonché l'attuazione di pratiche commerciali scorrette o predatorie. Il KOSA obbligherebbe, infatti, i prestatori di servizi digitali a introdurre *by design* misure “*ragionevoli*” ad evitare l'esposizione del minore di età a certi contenuti, come funzionalità che limitino l'accesso ad attività di ricerca di contenuti relativi ai menzionati scenari dannosi, o che evitino a terze parti di comunicare, visualizzare o processare dati personali degli utenti minorenni, o che incentivino lo svilupparsi di dipendenze, attraverso mec-

⁽²⁵⁾ FEDERAL TRADE COMMISSION, *A Six Step Compliance Plan for Your Business*, <https://www.ftc.gov/business-guidance/resources/childrens-online-privacy-protection-rule-six-step-compliance-plan-your-business#step2>.

⁽²⁶⁾ S.1409 - 118th Congress (2023-2024), <https://www.congress.gov/bill/118th-congress/senate-bill/1409/text>.

canismi di accesso automatico o premialità per la permanenza sulla piattaforma, attribuendo la gestione di tali profili e blocchi (come ad esempio quello relativo alla possibilità di compiere acquisti) direttamente ai genitori o agli educatori, a seconda dell'oggetto del servizio erogato. Una critica al concetto di “*techno-legal solutionism*” che funge da premessa al KOSA, muove dal fatto che si presume che le “piattaforme” danneggino direttamente i giovani e che una soluzione tecnologica sia sempre possibile, sulla base di una semplificazione dell'interpretazione di fenomeni sociali complessi — come il rapporto tra *social media* e salute mentale degli utenti. Dal punto di vista giuridico, il *techno-legal solutionism* avrebbe pertanto il limite di presumere il rapporto di causalità nell'interpretazione della diligenza (*standard of care*) dell'operatore economico ⁽²⁷⁾.

Anche laddove il Congresso non riuscisse a completare l'*iter* di approvazione di queste iniziative ⁽²⁸⁾, la riflessione è avviata e si alimenterà di ulteriori profili, considerata la decisione della Corte Suprema di non pronunciarsi in ordine alla compatibilità delle leggi statali della Florida e del Texas in materia di piattaforme di comunicazione di massa con il primo emendamento ⁽²⁹⁾.

Al livello statale, infatti, vi sono una pluralità di iniziative settoriali che hanno ricadute sull'uso da parte di soggetti minorenni di servizi della società dell'informazione o nuove tecnologie. Ai nostri fini, meritano menzione altre proposte, come quella presentata al Senato

⁽²⁷⁾ Così M. P. ANGEL, D. BOYD. *Techno-legal Solutionism: Regulating Children's Online Safety in the United States*. In Proceedings of 3rd ACM Computer Science and Law Symposium (CSLAW'24), 2024, ACM, Boston, MA, USA, 86 e ss. <https://doi.org/10.1145/3614407.3643705>. Sull'interpretazione del *duty of care* verso i bambini C. NYAMUTATA, *Childhood in the Digital Age: A Socio-Cultural and Legal Analysis of the UK's Proposed Virtual Legal Duty of Care* (2019) 27:4 Int'l JL & Info Tech 311.

⁽²⁸⁾ Nelle more della redazione di questo contributo il Senato ha approvato in prima lettura le due proposte, avanzando nell'*iter* di adozione in data 30 luglio 2024.

⁽²⁹⁾ Con una decisione presa all'unanimità la Corte Suprema ha rinviato ai giudici di merito, considerando che i limiti imposti dalle normative rispettivamente della Florida e del Texas in materia di *social media platforms* rispetto alla capacità delle stesse “di moderare i contenuti, ovvero di filtrare, dare priorità ed etichettare i vari messaggi di terze parti, video e altri contenuti che gli utenti desiderano pubblicare”, ovvero di fornire “spiegazioni individualizzate, che richiedono a una piattaforma di fornire motivazioni a un utente se rimuove o modifica i suoi post” non siano contrarie al primo emendamento. Supreme Court, Op. No. 22-277. Argued February 26, 2024- Decided July 1, 2024, https://www.supremecourt.gov/opinions/23pdf/22-277_d18f.pdf.

dello Stato della Florida ⁽³⁰⁾, che proibisce per i minori di anni sedici l'uso dei *social network* al pari di quanto era già stato approvato (e in seguito modificato) nello Stato dello Utah ⁽³¹⁾, che vietava di aprire *account* ai residenti minori di anni diciotto, a meno che non vi fosse un consenso del legale rappresentante, da esprimersi nei quattordici giorni successivi alla creazione del profilo. Anche nella nuova formulazione, la legge dello Utah prevede che i prestatori di servizi digitali debbano implementare una serie di meccanismi adeguati di identificazione e accertamento dell'identità, non essendo sufficiente l'esibizione del documento, in quanto ritenuto un mezzo facilmente aggirabile dai minori stessi, dovendo il titolare del trattamento garantire, peraltro, un livello di precisione rispetto ai meccanismi di verifica pari al 95%. Resta fermo, che la base giuridica per il trattamento delle informazioni personali del minore di età sia, in ogni caso, il consenso del genitore.

La normativa stabilisce l'obbligo di implementare strumenti di supervisione della navigazione, in ordine alla possibilità di impostare limiti di tempo, programmare pause e visualizzare determinate impostazioni nel profilo dell'utente, nonché di disabilitare quelle funzionalità atte a prolungare il coinvolgimento dei minori, tra cui i meccanismi di riproduzione automatica di contenuti, quelli di scorrimento infinito delle app e le notifiche cc.dd. *push* ⁽³²⁾.

Con riferimento alla sicurezza dei flussi di informazioni, inoltre, le piattaforme digitali devono prevedere impostazioni predefinite, quali:

⁽³⁰⁾ Florida Senate, *An act relating to social media use for minors*, s. 501.17362024 CS for SB 1788, <https://flsenate.gov/Session/Bill/2024/1788/BillText/c1/HTML>.

⁽³¹⁾ Utah Social Media Regulatory Act, Utah Code §§ da 13-63-101 a 701. Tuttavia, un'associazione di categoria rappresentante servizi digitali ha presentato un reclamo contro la nuova legge, sostenendone la contrarietà rispetto al primo e quattordicesimo emendamento. Il governo dello Utah ha quindi proposto una nuova normativa che abroga la prima e introduce alcuni correttivi, tra cui il diritto di azione per il risarcimento da danno causato dall'uso di piattaforme guidate dal algoritmi, così Social Media Amendments, HB 464, disponibile <https://le.utah.gov/~2024/bills/static/HB0464.html> and SB 194, <https://le.utah.gov/~2024/bills/static/SB0194.html>.

⁽³²⁾ Nella precedente formulazione, peraltro, si prevedevano direttamente fasce orarie in cui l'uso di *social media* era da considerarsi espressamente vietato (come nelle ore notturne) includendo, altresì, la possibilità di impostare un limite massimo di permanenza sulle piattaforme, sebbene con il correttivo di abilitare da parte dei genitori/legali rappresentanti funzioni che dessero maggiore autonomia al minore, laddove ricorressero specifiche necessità.

la limitazione della visibilità e indicizzazione da parte dei motori di ricerca dei profili dei minorenni, la limitazione delle interazioni attraverso condivisioni o messaggi solo agli *account* in quel momento collegati, lo sfruttamento dell'informazione relativa al minore, oltre quanto necessario per il funzionamento principale del servizio. Sul piano della trasparenza, infine, la nuova norma prevede di fornire idonea informativa sulla raccolta, uso e riuso delle informazioni, nonché di consentire — su richiesta del minore — la cancellazione d'ufficio di quanto (informazioni o materiali) reso pubblico dall'utente minorenne ⁽³³⁾.

Negli esempi riportati emerge con fermezza l'intento di individuare specifici obblighi ai prestatori di servizi digitali volti a promuovere un ruolo proattivo dei genitori e supportarli nell'esercizio delle relative responsabilità, affinché possano divenire (se già non lo siano) consapevoli delle implicazioni che l'uso, nella specie di *social media* può determinare nella gestione della quotidianità dei figli, adottando *by default* un approccio allo scopo di limitare la solitudine nelle attività digitali ⁽³⁴⁾ attraverso strumenti che inducano e sollecitino una supervisione o validazione da parte degli adulti.

Non dissimile la recente proposta australiana di modifica dell'attuale normativa in materia di protezione dell'ambiente digitale, volta a limitare l'uso dei social media agli infrasedicenni, stabilendo sanzioni per le piattaforme in caso di mancata introduzione di strumenti di verifica dell'età degli utenti ⁽³⁵⁾. Nel *report* della commissione parlamentare ⁽³⁶⁾ sono illustrati i risultati della consultazione che ha visto esprimersi anche l'*E-safety Youth Commission*, che ha espresso perplessità circa l'efficacia della proposta volta a proibire l'accesso alle

⁽³³⁾ Sia concesso rinviare a D. AMRAM - N. PATTI, *Recent Policy Initiatives and Safeguards for Children as Online Users*, IDC 2024 Conference, Delft 17.06.2024.

⁽³⁴⁾ A incrementare il rischio di incorrere in un pericolo per la sicurezza o incolumità online è infatti il dato relativo alla permanenza senza supervisione e generalmente in solitaria del bambino, così UNICEF, *The State of the World's Children 2017: Children in a digital world*, 2018, <https://www.unicef.org/eap/press-releases/more-175000-children-go-online-first-time-every-day-tapping-great-opportunities>.

⁽³⁵⁾ Online Safety Amendment (Social Media Minimum Age) Bill 2024, cit. Cap.1 §9.

⁽³⁶⁾ Joint Select Committee on Social Media and Australian Society, *Social media: the good, the bad, and the ugly. Final Report*, November 2024.

risorse digitali, argomentando la propria posizione sottolineando il ruolo della costruzione di un ambiente digitale sicuro investendo sui percorsi educativi e formativi ⁽³⁷⁾. Di contro, la proposta consentirebbe di evitare una condivisione anche inconsapevole di una varietà di informazioni a scopi commerciali che vengono raccolte e trattate attraverso la navigazione sui *social media*, tra cui i dati biografici, l'immagine, la voce, la risposta cerebrale agli stimoli, nonché dati demografici sulla loro identità e sul relativo nucleo familiare ⁽³⁸⁾.

Questa prospettiva di protezione, in assenza di bilanciamenti e contemperamenti, rischia tuttavia di entrare in tensione rispetto all'interesse superiore del bambino a rendersi progressivamente autonomo nelle attività quotidiane. Appare però ragionevole imporre gli strumenti che consentano — a discrezione del genitore — di rappresentare gli interessi del bambino, ovvero supervisionarli e/o validarli, fino a validarli solo su richiesta, consentendo di incrementare progressivamente gli spazi di autonomia dell'utente adolescente in ragione di un equilibrato esercizio delle responsabilità genitoriali. La sfida è, pertanto, quella di identificare i parametri per interpretare la maturità del singolo utente e ridurre le forme di controllo.

Su questa scia, un'iniziativa che merita attenzione è quella promossa dallo Stato di New York, che appare prendere in considerazione il bilanciamento tra protezione dall'esposizione a rischi e la compromissione della libertà di espressione che un divieto di accesso comporterebbe, proponendo nell'Online Safe Kids Act dell'agosto 2024 che le piattaforme *social media* siano tenute a utilizzare “*metodi commercialmente ragionevoli e tecnicamente fattibili*” per determinare l'età del-

⁽³⁷⁾ “*Relevant and comprehensive education should be readily accessible and focus on supporting young people and families to encourage open dialogue to develop digital literacy, online safety skills, and help-seeking behaviours suited to each young person. Age verification tools cannot account for evolving maturity levels and differing capabilities among young people the way education can*”, eSafety Youth Council, *Submission* 60, p. 3.

⁽³⁸⁾ “*we should regulate to ban the harvesting, sale and exchange of all children's data for commercial use, including their biodata and their neural data. That includes their image, their voice and their brain response to stimuli as well as demographic data about who they are, where they live, who their parents are, how old they are and what gender they are*”, Ms Sarah Davies, Chief Executive Officer, Alannah and Madeline Foundation, *Proof Committee Hansard*, 10 July 2024, p. 46.

l'utente, prima di fornirgli contenuti (*feed*) che possano creare dipendenza, fatto salvo che il genitore abbia prestato il proprio consenso ⁽³⁹⁾.

L'età non costituirebbe, dunque, un limite all'accesso al servizio, ma alla proposizione di contenuti nocivi in quanto il c.d. *addictive feed* è "*parte significativa dei servizi*" della piattaforma, fatta eccezione per le funzionalità di personalizzazione impostate dall'utente che riguardino l'accessibilità o la *privacy* o informazioni tecniche sul dispositivo dell'utente. La proposta mira, pertanto, a proteggere la salute dei minori di età rispetto allo specifico rischio correlato allo sviluppo di dipendenze dovuto allo sfruttamento a fini commerciali dei dati e dei comportamenti degli utenti minorenni attraverso algoritmi.

3.2. *Le misure a portata dei bambini dell'Online Safety Act: il pragmatismo britannico.*

Come accennato nel capitolo precedente, il Regno Unito si è dotato nell'autunno 2023 di una normativa per un ambiente digitale sicuro, l'Online Safety Act (di seguito anche "OSA"), con l'espresso obiettivo di introdurre obblighi affinché i prestatori di servizi digitali gestiscano i rischi relativi alla diffusione di contenuti illeciti o pregiudizievoli, prestando particolare attenzione al sistema di tutele per i minori di età ⁽⁴⁰⁾. Con un approccio pragmatico si enuncia il principio di *safety by design*, prioritarizzando gli interventi di attuazione secondo tre direttive: quella di proteggere con *standard* più robusti i minori di età rispetto agli adulti, quella di promuovere la libertà di espressione e la *privacy* degli utenti, e quella di osservare i principi informatori della materia, ovvero quelli di trasparenza e *accountability*.

L'intervento normativo distingue i servizi *user to user* da quelli di ricerca a seconda che i contenuti possano essere visibili ad altri utenti

⁽³⁹⁾ SAFE for Kids Act, *Advanced Notice of Proposed Rulemaking pursuant to New York General Business Law section 1500 et seq*, 1 agosto 2024, <https://ag.ny.gov/sites/default/files/2024-08/safe-forkidsact.pdf>.

⁽⁴⁰⁾ Nell'aprile 2019 era stato pubblicato il Libro bianco sui pregiudizi online che dopo molteplici iterazioni era confluito Online Safety Bill (OSB), pubblicato nella sua forma originale nel maggio 2021, e infine approvato come Online Safety Act, entrato in vigore il 26 ottobre 2023, https://www.legislation.gov.uk/ukpga/2023/50/pdfs/ukpga_20230050_en.pdf. M. TRENGOVE, E. KAZIM, D. ALMEIDA, A. HILLIARD, S. ZANNONE, E. LOMAS, *A critical review of the Online Safety Bill*, Patterns (N Y). 2022 Jun 24; 3(8):100544. doi: 10.1016/j.patter.2022.100544. PMID: 36033594; PMCID: PMC9403395. Si veda la ricostruzione sistematica di S. RIGAZIO, *L'empowerment del minore nella dimensione digitale*, Mucchi editore, 2024.

o meno. Per entrambi richiede ai prestatori di servizi digitali di osservare lo stesso *standard* rispetto al *duty of care* riguardo alla gestione di contenuti illeciti, alle attività di segnalazione, alla gestione dei reclami, all'attuazione della libertà di espressione e della riservatezza e alla documentazione delle analisi dei rischi effettuate.

Tale valutazione deve essere utente-centrica e analizzare ciascun pericolo separatamente dagli altri, secondo ordini di priorità stabiliti dalla norma. In particolare, in primo luogo, saranno presi in considerazione i pericoli cc.dd. prioritari, come quello di terrorismo, di sfruttamento sessuale e abuso di minori, e di reati considerati più gravi. Dopodiché, la valutazione può proseguire ad analizzare le esposizioni ad altre tipologie di illeciti. Occorre tener conto, tra le altre, dell'uso di algoritmi che possano incrementare la riproduzione del contenuto, delle funzionalità della piattaforma, della tipologia e dei possibili usi dei servizi digitali, della natura e gravità dei pregiudizi, nonché l'impatto del *design* e del funzionamento del servizio (inclusi il modello di *business*, le tecnologie proattive, la *governance* dei flussi e il livello di alfabetizzazione e consapevolezza).

Questo sistema di tutele trova spazio laddove sia “*verosimile che il servizio digitale sia utilizzato da minori*” ⁽⁴¹⁾. In particolare, gli articoli 11, 12 e 13 OSA affrontano le modalità di ottemperare rispettivamente agli obblighi di valutazione del rischio, di sicurezza verso i minori e della relativa interpretazione. In particolare, la valutazione deve svilupparsi seguendo uno *standard* definito “*adeguato e sufficiente*”, nei tempi normativamente previsti, e deve essere documentata. La stessa deve, inoltre, essere commisurata alle caratteristiche degli utenti, considerando il numero per fasce di età rappresentate e riguardare le parti delle piattaforme accessibili ai minori di età. I livelli di indagine devono riferirsi — sempre separatamente — ai diversi pericoli cui sono esposti gli utenti minori di età, procedendo, come anticipato, a valutare dapprima quelli a cui è assegnata una pericolosità di tipo primaria e prioritaria — ovvero quelli che mostrino contenuti pornografici, o che istighino al suicidio o ad atti di autolesionismo, o inducano a disordini alimentari — proseguendo, poi, con l'analisi dei pericoli relativi all'esposizione a contenuti discriminatori o a discorsi d'odio, o a con-

(41) Ovvero — come esplicitato all'art. 37 — se la circostanza sia stata accertata attraverso una verifica degli accessi, o il prestatore si sia reso inadempiente rispetto all'obbligo di verifica degli accessi ovvero la circostanza sia risultata da un'istruttoria dell'autorità competente.

dotte di bullismo ⁽⁴²⁾, o violenza contro persone o animali (simulati o meno), o che promuovano sfide o giochi pericolosi per l'incolumità psicofisica, o che inducano a ingerire, iniettare o inalare sostanze velenose ⁽⁴³⁾.

Per ciascuna fascia di età rappresentata, la valutazione deve tener conto anche delle ulteriori vulnerabilità, come quelle determinate dall'appartenenza del singolo ad un determinato gruppo o all'impatto derivante da alcuni elementi caratterizzanti l'utente, considerato come individuo.

Rispetto alle funzionalità di sistema, sono ritenute ad elevato rischio quelle che consentono a soggetti adulti di ricercare e interagire coi minori. Con riferimento all'uso, sono altrettanto pericolosi quei meccanismi che incentivino la permanenza *online*. Nel primo caso, infatti, il pericolo riguarda l'esposizione a furti di identità o ai rischi legati all'adescamento, mentre nel secondo caso, allo sviluppo di disordini e dipendenze.

L'articolo 12 enuncia i cc.dd. *duty of safety* da osservare in tutti i servizi che siano verosimilmente utilizzati dai minori di età, rispetto alla progettazione (*by design*) e abilitazione (*by default*), volte ad introdurre misure per mitigare e gestire i rischi e ridurre gli effetti pregiudizievoli. In particolare, si stabilisce la necessità di implementare misure che siano proporzionate ad evitare al minore di incorrere in contenuti di pericolosità primaria e prioritaria, e di proteggere coloro che siano più sensibilmente esposti. Potrebbe occorrere non solo un sistema di verifica dell'età, ma anche di stima della stessa, emergendo dalla prassi la facilità con cui il requisito formale dell'anno di nascita possa essere aggirato. Per tale ragione, al fine di evitare al minore di età di entrare in contatto con pericoli a priorità primaria e prioritaria, il prestatore di servizi digitali può limitare l'accesso a particolari contenuti, moderarli, bloccare funzioni o assumerne il controllo, dovendo peraltro supportare l'utente a gestire l'esposizione. I termini e le condizioni d'uso del servizio devono, in ogni caso, rendere note le misure di protezione introdotte, le modalità di gestione dei pericoli, come sopra definiti, e fornire supporto all'utente che — nonostante le misure implementate — si trovi di fronte a contenuti dannosi considerati di livello di rischio

⁽⁴²⁾ Per bullismo si intendono condotte che trasmettano una grave minaccia, umilianti o degradanti, facenti parte di una campagna di maltrattamenti.

⁽⁴³⁾ Per contenuto si intendono stringhe di testo o testo accompagnato da GIF, emoji o altro simbolo, ovvero relative combinazioni.

primario e prioritario, ovvero subisca pregiudizi per quei contenuti che non erano stati considerati di tale impatto in sede di analisi dei rischi. I documenti informativi devono altresì riportare specifiche tecniche in ordine alle tecnologie utilizzate per conformarsi agli obblighi di protezione e le risultanze della valutazione di impatto devono poter essere rese accessibili ⁽⁴⁴⁾.

L'interpretazione dell'estensione del c.d. *duty of safety* è demandata all'art. 13 OSA che introduce in termini di proporzionalità dei correttivi all'assolutezza degli obblighi descritti nel precedente articolo 12. In particolare, si specifica che la conformità al menzionato obbligo è commisurata alle più recenti evidenze sulla valutazione del rischio per i bambini, da un lato, e all'estensione e capacità del prestatore di servizi, dall'altro.

Il pregio dell'OSA risiede proprio nell'accompagnare i fornitori di servizi digitali nella valutazione di impatto predeterminando i piani su cui misurare le vulnerabilità, i pericoli di esposizione e i rischi per le diverse fasce di età. D'altro canto, appare verosimile che tale approccio richieda un aggiornamento costante in ragione della continua evoluzione delle tecnologie utilizzate. Il richiamo alla valutazione dei rischi sulla base del relativo stato dell'arte potrebbe infatti a breve vanificare lo sforzo di articolare una metodologia efficace di analisi dei rischi. In ogni caso, resta di gran lunga lo strumento normativo più capace di rendere l'ambiente digitale sicuro e alla portata delle vulnerabilità rappresentate dagli utenti minori di età.

Ulteriore limite appare quello di riferirsi esclusivamente ai servizi digitali, si potrebbe auspicare che la sensibilità normativa del Regno Unito si manifesti anche rispetto alla regolamentazione dei sistemi basati sull'IA utilizzando il medesimo approccio.

In questo contesto, appare pregevole l'iniziativa dell'autorità garante per i dati personali del Regno Unito, l'ICO, che — parallelamente — promuove nell'ambito del codice di condotta per i servizi digitali, una campagna specifica per una cultura digitale a portata dei minori, coinvolgendo figure chiave dell'economia del paese, come dirigenti, *manager* e consulenti aziendali, nonché i volontari e operatori di organizzazioni *no-profit*, funzionari pubblici, etc. in attività di formazione e acquisizione di competenze specifiche volte a responsabilizzare

⁽⁴⁴⁾ P. COE, *Tackling Online False Information in the United Kingdom: The Online Safety Act 2023 and its Disconnection from Free Speech Law and Theory*, in *Journal of Media Law*, 2024 <https://doi.org/10.1080/17577632.2024.2316360>.

la società civile a prestare attenzione alle vulnerabilità dei minori nell'ambiente digitale ⁽⁴⁵⁾.

Emerge in questa iniziativa l'approccio *lato sensu* europeo, che conferma la virtuosa attitudine dell'ICO a tradurre in buone prassi operative i principi informatori della strategia EU dei dati (*accountability, fairness, transparency*) ⁽⁴⁶⁾, continuando — nonostante la *brexite* — a investire nell'obiettivo a lungo termine di cambiamento culturale per la costruzione di ambienti digitali sicuri e affidabili, attraverso la collaborazione con gli operatori (aziende private, istituzioni e più in generale la società civile). Non vengono dunque sanciti obblighi specifici per i genitori (o legali rappresentanti) rispetto agli obblighi generali di educazione, cura e mantenimento della prole, ma si incentiva la responsabilizzazione degli adulti, ciascuno per il proprio ruolo nella società, contribuendo a costruire un sistema multilivello di responsabilità.

3.3. *La riforma cinese e l'autonomia c.d. limitata.*

Come osservato in precedenza, nell'ottobre del 2023, la Cina ha introdotto delle norme a tutela dei minori di età nello spazio digitale ⁽⁴⁷⁾ a completamento delle disposizioni specifiche in materia di tutela dei dati personali ⁽⁴⁸⁾ e in ottica di sistematizzazione della normativa a carattere generale sulla tutela dei minori e sulla cybersicurezza ⁽⁴⁹⁾. Nei mesi antecedenti l'approvazione, il dibattito si era concentrato sulla necessità di prendere in considerazione le problematiche comuni a categorie di soggetti vulnerabili, legate alla personalizzazione della protezione del singolo, nonché sull'opportunità di indi-

⁽⁴⁵⁾ ICO, *Age appropriate design: a code of practice for online services*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>.

⁽⁴⁶⁾ Sin dall'entrata in vigore del GDPR l'ICO ha svolto un ruolo essenziale di sviluppo di linee guida e prassi, *Guidance and resources*, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>.

⁽⁴⁷⁾ Regolamento sulla protezione dei minori in Internet, 24 ottobre 2023, in vigore dal giorno 1 gennaio 2024, disponibile https://www.cac.gov.cn/2023-10/24/c_1699806932316206.htm.

⁽⁴⁸⁾ Children Information Provisions, 2019.

⁽⁴⁹⁾ Tali disposizioni sono confluite negli artt. 28 e 31 del Personal Information Protection Law of the P. R. China (PIPL), 29 agosto 2021, non presenti nelle prime versioni.

viduare un efficace bilanciamento tra rischi della digitalizzazione e lo sfruttamento di opportunità paritarie.

Il recente intervento regolatorio si propone di fornire linee guida per la gestione e protezione delle informazioni riguardanti i bambini nell'ambiente digitale, dando attuazione alla norma contenuta nella legge sulla protezione dei dati che classifica di natura sensibile le informazioni relative a soggetti infraquattordicenni, con conseguenti implicazioni sulle modalità di raccolta e acquisizione del consenso del genitore a fini del relativo trattamento, incluso l'obbligo di formulare informative specifiche per i soggetti minori di età ⁽⁵⁰⁾. In particolare, si ritiene che laddove il consenso sia base giuridica del trattamento di dati di minori di anni quattordici sia necessaria la forma scritta, ovvero una condotta separata (e specifica) rispetto all'accettazione dei termini e condizioni d'uso del servizio da parte del genitore, non essendo sufficiente l'acquisizione generica.

L'introduzione di procedure complesse per la raccolta del consenso non appare in ogni caso un meccanismo efficace a tutelare i giovani utenti rispetto ai reali rischi di profilazione e perdita del controllo delle informazioni, essendo — secondo i commentatori ⁽⁵¹⁾ — preferibile introdurre specifici divieti di uso e riuso delle informazioni *by design*, come avviene nel DSA, anziché formalità facilmente aggirabili dagli utenti stessi. Occorre rilevare che nel codice civile cinese i minori che abbiano compiuto gli otto anni di età sono considerati soggetti a “*incapacità limitata*”, presi in considerazione alcuni fattori (età, salute mentale e capacità cognitive del singolo), possono addirittura compiere atti giuridici che perseguano l'interesse superiore dell'interessato. Diventa dunque dirimente disporre di strumenti di verifica e accertamento sia dell'età dell'utente, che della capacità di discernimento. Spetta infatti al titolare del trattamento provare che l'infraquattordicenne rientri nella riserva di cui all'art. 145 del codice civile cinese, viceversa spetta al genitore provare che il

⁽⁵⁰⁾ L. ZHANG, K. KOLLNIG, *Theory and practice: the protection of children's personal information in China*, in *International Data Privacy Law*, Volume 14, Issue 1, February 2024, p. 37 ss., <https://doi.org/10.1093/idpl/ipad017>. In particolare, vista la collocazione della norma, tutte le misure di salvaguardia previste per i dati sensibili sono applicabili in caso di soggetto interessato minore di anni quattordici, con conseguente obbligo per il titolare del trattamento di verificare l'età dell'utente.

⁽⁵¹⁾ *Ibidem*, p. 46.

minore che abbia compiuto quattordici anni non fosse comunque capace di esprimere un consenso valido per un determinato atto ⁽⁵²⁾.

In questo quadro, l'art. 5 del nuovo regolamento attribuisce alle scuole e alle famiglie il compito di “*educare e guidare i minori*” ad un uso benefico di *internet* utilizzandolo in “*modo scientifico, civile, sicuro e ragionevole*”, intervenendo contro fenomeni di dipendenza.

Inoltre, un intero capitolo della normativa è dedicato all'alfabetizzazione. In particolare, spetta al dipartimento dell'istruzione sostenere programmi di educazione digitale volti a sviluppare una “*consapevolezza morale*” e una conoscenza degli strumenti tecnici e giuridici per l'utilizzo dello spazio digitale in ottica di protezione della sicurezza personale e patrimoniale e, in particolare, dei minori di età. Ulteriori disposizioni, poi, richiamano la necessità di allestire in spazi pubblici postazioni con *software* aggiornati e misure di protezione per una navigazione sicura, includendo la previsione di personale qualificato e volontari al servizio dei bambini utenti. In particolare, l'art. 16 si rivolge alle istituzioni scolastiche, specificando la necessità di adeguare strutture e programmi alle sfide della digitalizzazione, onde consentire una più ampia accessibilità.

Nell'ambito della promozione della ricerca e sviluppo dei servizi della società dell'informazione a misura di bambini, l'art. 18 stabilisce, da un lato, che sono punite tutte le attività che possano ledere la salute fisica e mentale dei minori e, dall'altro, che lo Stato si obbliga a rendere sicuro e salutare l'ambiente digitale, come impegno contro forme di dipendenza, nonché a renderlo un ambiente più inclusivo capace di valorizzare le attitudini e i talenti dei minori ⁽⁵³⁾.

L'art. 19 introduce un principio di protezione *by design* per i sistemi utilizzati dai minori, mentre l'art. 20 si rivolge alle piattaforme digitali utilizzate “*da un gran numero di minori*” o che abbiano “*un impatto significativo*” su gruppi di minori di età, prevedendo un approccio del tutto simile a quello illustrato nel DSA, arricchito

⁽⁵²⁾ Si consideri che anche in Cina la maggiore età coincide con il compimento di diciotto anni, ma che in seno agli artt. 19 e 145 del Codice civile cinese, i bambini che abbiano compiuto gli otto anni possono avere una seppur limitata capacità per atti giuridici stipulati nel loro esclusivo interesse.

⁽⁵³⁾ Ciò in linea con quanto stabilito dall'art. 13, Cybersecurity Law of the People's Republic of China, disponibile <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/#:~:text=Any%20person%20and%20organization%20using,interests%3B%20they%20must%20not%20incite.>

tuttavia di elementi pratici utili alla discussione sulla valutazione di impatto. Si richiede, infatti, agli operatori di valutare continuamente, sia in sede di progettazione, che di ricerca e sviluppo, che di funzionamento etc. i rischi per la salute fisica e mentale dei minori di età, in osservanza della normativa di settore, nonché di identificare modalità per erogare servizi o utilizzare prodotti in maniera sicura per i bambini. In mancanza, ovvero in caso di pregiudizio psicofisico o compromissione di altri interessi legittimi dei minori di età, vi è un obbligo di interrompere l'erogazione del servizio o la fornitura del prodotto. Inoltre, si prevede lo stabilimento di una autorità garante con competenze di controllo e supervisione circa l'effettivo uso da parte dei minori dei servizi della società dell'informazione anche attraverso l'analisi delle attività obbligatorie di reportistica previste dal medesimo articolo.

L'art. 22 pone una serie di divieti per le persone fisiche o giuridiche. In particolare, si proibisce la produzione, copia, pubblicazione o diffusione di contenuti che promuovano *“l'oscenità, la pornografia, la violenza, le sette, la superstizione, il gioco d'azzardo, inducono all'autolesionismo e al suicidio, al terrorismo, al separatismo, all'estremismo, ecc. che mettono in pericolo la salute fisica e mentale salute dei minori”*, incluso materiale pedopornografico.

L'art. 23 prevede un bilanciamento rispetto alla produzione o pubblicazione di contenuti pericolosi per la salute psicofisica del minore in quanto potrebbero indurre a imitare comportamenti non sicuri, non etici, o a produrre emozioni estreme, o a sviluppare cattive abitudini, stabilendo in questi casi un obbligo di avvisare l'utenza con una informativa ben visibile. Ciò vale anche per i contenuti accessibili con mezzi di comunicazione di massa e per il settore editoriale, cinematografico e turistico. Inoltre vieta pratiche di profilazione a fini di *marketing*.

L'art. 26 definisce e proibisce pratiche riconducibili al cyberbullismo come effetto di contenuti pubblicati online al fine di *“umiliare, diffamare, minacciare o danneggiare maliziosamente l'immagine di minori attraverso l'uso di testi, immagini, audio e video”* etc., invitando i fornitori di servizi ad impostare meccanismi di *alert* e reportistica immediata. L'impostazione preferibile appare essere quella di selezionare opzioni di protezione delle informazioni relative al cyberbullismo *by design* che portino in via preventiva a bloccare utenti non familiari, informazioni pubblicate, ovvero la possibilità di condividere o estendere la pubblicazione o commentare i contenuti illeciti. Più in generale

si invitano i fornitori di servizi digitali a sviluppare tecniche, anche basate sull'IA e validate manualmente, per identificare contenuti e profili e procedere ad una efficace lotta al *cyberbullismo*.

L'art. 29 è altrettanto interessante dal punto di vista pratico in quanto elenca una serie di misure volte a punire i fornitori di servizi digitali in caso di contenuti posti o distribuiti in violazione delle misure di protezione di cui ai precedenti articoli. In particolare, sono adottate misure chiamate "*di smaltimento, quali la cancellazione, il blocco e la disconnessione*" volte ad impedire la proliferazione delle informazioni, è istituito un registro di segnalazione alla sicurezza informatica, alla pubblica sicurezza e ad altri dipartimenti affinché possano ricevere avvisi, limitare le funzioni, sospendere servizi, chiudere *account* e altre misure di "*smaltimento*" per gli utenti: in tal modo i contenuti illeciti saranno non solo bloccati e distrutti, ma anche i profili ad essi collegati saranno sospesi.

Le esperienze nazionali descritte costruiscono sistemi complessi multilivello in cui misure di salvaguardia di natura diversa possono trovare contestuale applicazione da parte di attori diversi per una più efficiente protezione della persona e dei suoi diritti.

4. La protezione dei fanciulli *by design* e il ruolo degli *standard tecnici*.

Come osservato nel capitolo precedente, sia il Consiglio d'Europa, che la Commissione Europea hanno lanciato strategie sui diritti dell'infanzia che comprendono specifiche garanzie rivolte alla digitalizzazione e all'uso dell'intelligenza artificiale, affinché si possano definire le condizioni per un ambiente digitale sicuro e resiliente, alla portata dei minori, attraverso la promozione di misure di salvaguardia da parte dei fornitori di servizi, dei genitori e degli operatori sanitari e di tutte le parti interessate.

Se assicurare una libera ed efficace circolazione dei flussi di dati personali costituisce uno degli obiettivi cardine della strategia europea dei dati personali e non personali al fine di promuovere in ogni settore le potenzialità offerte dalla società dell'informazione, occorre investigare come siano declinati i diritti fondamentali del fanciullo nella dimensione digitale per comprendere non solo quali misure di salvaguardia introdurre per la loro tutela, ma altresì su quali elementi abilitatori far leva, per incoraggiare uno sviluppo psicofisico armonico

rispetto all'evoluzione della società, raggiungendo più alti livelli di benessere.

Abbiamo visto come il mancato raggiungimento della maggiore età costituisca per certi profili una vulnerabilità mitigata in quanto il quotidiano uso dei servizi della società dell'informazione — per lo più gratuiti — da parte di minorenni, ha portato i legislatori a introdurre misure di contemperamento per valorizzare l'autonomia degli adolescenti, che acquisiscono quotidianamente — se educati ad un uso responsabile — competenze e abilità per fruire dei servizi digitali in maniera sicura, al pari di certi adulti. Infatti, l'esposizione ad alcuni rischi legati a condotte illecite di terzi, ovvero a inferenze sul comportamento (come lo sviluppo di forme di dipendenza) o sulla libera formazione del pensiero critico possono infatti essere comuni anche agli adulti: ed è solo con la collaborazione dei genitori e attraverso una idonea formazione che l'esposizione ai pericoli può essere efficacemente mitigata.

Si pensi alle ricadute future del furto dell'identità digitale di un bambino: non è detto che gli effetti pregiudizievoli si manifestino subito o siano percepibili dal minore o dagli adulti di riferimento, non è chiaro fino a che punto ci possano essere implicazioni un domani rispetto all'eventuale esposizione a un pericolo oggi.

In questo contesto, proteggere i diritti fondamentali del minore nella dimensione digitale appare un'operazione tutt'altro che semplice: taluni sistemi hanno adottato un atteggiamento difensivo, volto a limitare e/o proibire l'uso della tecnologia sino ad una certa età, al fine di evitare il più possibile l'esposizione ai rischi, il che — tuttavia — si scontra, come abbiamo visto, con il dato reale che vede bambini tra gli utenti più attivi della società dell'informazione ⁽⁵⁴⁾ e con l'interesse superiore a rendere i giovani partecipi della dimensione digitale e delle relative opportunità ⁽⁵⁵⁾. Per altri sistemi, invece, si tratta di distribuire il rischio tra operatori economici e adulti di riferimento (genitori, educatori etc.) e indicare chi debba essere onerato della valutazione

⁽⁵⁴⁾ UNICEF, *The State of the World's Children 2017: Children in a digital world*, cit.

⁽⁵⁵⁾ V. SCALISI, *Superiore interesse del minore ovvero il fatto come diritto*, in Riv. dir. civ., 2018, I, p. 407 e J. DOEK, 'Child Participation', in J. TODRES - M. K. SHANI (eds), *The Oxford Handbook of Children's Rights Law*, Oxford Handbooks (2020; online edn, Oxford Academic, 7 May 2020), <https://doi.org/10.1093/oxfordhdb/9780190097608.013.14>.

d'impatto di ogni applicazione sviluppata, distribuita, acquistata sul singolo utente minore di età. Conseguentemente, laddove il pericolo si verifichi, occorre ricostruire il sistema di *governance* per individuare la falla nelle misure di mitigazione e accertare le relative responsabilità.

La protezione dei minori di età nella dimensione digitale muove dal concetto di sicurezza da declinarsi nella società dell'informazione, non solo con misure tecniche, ma anche con quelle organizzative, che possono trovare nella proceduralizzazione dei meccanismi di mitigazione delle diverse tipologie di pericolo, secondo i relativi indici di serietà e occorrenza, gli opportuni bilanciamenti al fine di determinare la strategia più appropriata per la prevenzione dei rischi.

Nel ciclo di vita dello sviluppo di un prodotto o di un servizio digitale destinato al minore di età, pertanto, occorrerà introdurre elementi che consentano di agire in ottica preventiva e non rimediale. Si tratta di una operazione più semplice da gestire dal punto di vista tecnico, ma meno immediata laddove si consideri l'impatto positivo atteso dalla singola soluzione sui processi di crescita del minore.

Se in termini di sicurezza informatica tecniche *privacy-preserving* sono capaci di gestire flussi e accessi, identificare usi impropri e anomalie, occorre che le stesse siano comuni e condivise: pertanto dovranno essere oggetto di armonizzazione e standardizzazione tanto le regole di attivazione e disattivazione di ciascuna funzionalità, quanto le procedure di implementazione delle stesse. In particolare, lo sviluppatore dovrà disegnare una *governance* capace non solo di resistere agli impatti dei rischi noti e propriamente mitigati, ma anche di limitare eventuali conseguenze negative rispetto a quelli non noti o al verificarsi del pericolo nonostante l'implementazione di misure di salvaguardia.

A tal proposito, alcuni documenti sono stati pubblicati da associazioni di settore, volti a guidare gli sviluppatori in procedure e *checklist* che possano identificare livelli minimi di sicurezza in ottica, almeno, di *accountability* e diligenza al livello tecnologico.

Ad esempio, l'Institute of Electrical and Electronics Engineers (*alias* IEEE) ha recentemente riconosciuto degli *standard*, IEEE 2089-2021, che forniscono indicazioni per sviluppare procedure responsabili per sistemi rivolti a minori di età ⁽⁵⁶⁾. In linea di principio, il sistema deve poter riconoscere l'età dell'utente in maniera accurata tale da non

⁽⁵⁶⁾ IEEE, *Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*, in IEEE Std 2089-2021, vol., no., pp.1-54, 30 Nov. 2021, doi: 10.1109/IEEESTD.2021.9627644.

confondere il minorenni dal giovane adulto. Ancora, le interfacce di dialogo del sistema — e dunque i termini d'uso dello stesso e le informative — devono essere comprensibili ad un'utenza minore di età. Infine, occorre concretizzare attraverso specifiche funzioni di validazione dei processi decisionali automatizzati applicati all'utente del sistema, la prioritizzazione dell'interesse superiore dei fanciulli rispetto a qualsiasi altro interesse di tipo economico o commerciale.

Gli *standard* tecnici hanno il pregio di essere riconosciuti dalla comunità scientifica come applicabili a prescindere dal quadro giuridico di riferimento e, pertanto, godono di una rilevanza transfrontaliera fintanto che non sono sostituiti o aggiornati dall'evoluzione delle conoscenze tecniche in materia. Per tale ragione, nell'ambito della nostra riflessione — che si propone di formulare un modello di protezione e promozione dei diritti dei minori di età nella dimensione digitale suscettibile di trovare applicazione in una pluralità di esperienze giuridiche partendo dal carattere universale e condiviso delle vulnerabilità percepite e delle relative esposizioni — aderire a misure tecniche riconosciute come *standard* assume rilevanza giuridica in termini di valutazione delle condotte degli sviluppatori sia a fini di *accountability* rispetto all'espletamento degli obblighi di conformità alla normativa di settore, sia per — ad esempio — invertire l'allocazione di oneri probatori, potendo l'aderenza integrare una presunzione di diligenza in caso di pregiudizi. Un limite resta, tuttavia, ancorare le presunzioni di conformità al solo dato anagrafico, dovendo piuttosto poter individuare il grado di alfabetizzazione e capacità di discernimento.

Un altro esempio di armonizzazione e pre-standardizzazione è costituito dall'International Telecommunications Union che ha pubblicato nel 2020 una serie di linee guida destinate a genitori ed educatori, per *policy-maker* e per industrie in materia di sicurezza *online* per bambini ⁽⁵⁷⁾. Mentre le prime ⁽⁵⁸⁾ mirano a creare, da un lato, una interazione tra figli e genitori al fine di supportare un uso responsabile dei servizi della società dell'informazione, ammonendo a tenere sotto controllo i tempi di permanenza *online* e l'uso di carte di credito,

⁽⁵⁷⁾ ITU, *Child Online Protection Guidelines*, 2020, <https://www.itu-cop-guidelines.com/>.

⁽⁵⁸⁾ ITU, *Guidelines for Parents and Educators on Child Online Protection*, 2020, https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_f8a17ad2a3b94490add9a586ce4b6db8.pdf.

dall'altro lato, a fornire una sorta di *checklist* per un uso appropriato e disciplinato delle tecnologie nell'ambiente scolastico; quelle rivolte alle industrie ⁽⁵⁹⁾ sono più dettagliate e spiegano cinque aree di intervento. La prima riguarda la necessità di integrare le considerazioni sui diritti dell'infanzia in modo appropriato alle politiche aziendali e ai processi gestionali, la seconda concerne lo sviluppo di *standard* e procedure per gestire l'esposizione a materiali pornografici o vietare la creazione di quelli pedopornografici, come il blocco di *url* aventi contenuti *live*, ovvero l'oscuramento di contenuti illeciti. Oltre che responsabilizzare sulla funzione di moderazione dei contenuti per prevenire condotte manipolative o di *grooming* da parte di adulti, la terza area di intervento invita le industrie a promuovere un ambiente digitale più sicuro e appropriato all'età degli utenti anche da un punto di vista commerciale. Educare ad un uso responsabile dei servizi della società dell'informazione è visto, in attuazione del principio di alfabetizzazione, come quarta area di impegno verso gli utenti minori di età, genitori ed educatori. Infine, l'ultima linea di intervento riguarda la promozione della tecnologia digitale come strumento per incrementare il senso civico attraverso percorsi partecipativi che coinvolgano minori di età.

Le linee guida dedicate ai *policy maker* ⁽⁶⁰⁾, invece, introducono una *checklist* per elaborare una efficace strategia nazionale, che parta da una revisione della normativa esistente e si diriga verso strategie multilivello che coinvolgano le parti interessate, anche promuovendo forme di autoregolamentazione (come codici di condotta), incentivando lo sviluppo di meccanismi di reclamo per eventuali condotte improprie o pregiudizievoli, assieme alla promozione di campagne di sensibilizzazione per la cittadinanza e per gli operatori economici.

Queste ultime indicazioni contribuiscono a interpretare alcuni obblighi normativi e a promuovere un atteggiamento responsabile di tutti gli attori coinvolti verso le problematiche che concernono la tutela dei diritti dei minori di età nell'ambiente digitale. In particolare le indicazioni per le industrie richiamano la necessità di interventi coordinati per rendere il mercato a portata dei minori di età e non solo la singola applicazione.

⁽⁵⁹⁾ ITU, *Guidelines for industry on Child Online Protection*, https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_967b2ded811f48c6b57c7c5f68e58a02.pdf.

⁽⁶⁰⁾ ITU, *Guidelines for Policy Makers on Child Online Protection*, https://www.itu-cop-guidelines.com/_files/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf.

5. La valutazione di impatto con le lenti dei diritti dell'infanzia e il problema tecnico della verifica dell'età.

Se nell'ambiente fisico i prodotti destinati ai minori di età — come i giocattoli — possono essere pericolosi per la sicurezza e la salute, in ragione dell'esposizione a usi non conformi, la stessa cosa vale anche in ambiente digitale. La differenza è che l'origine dell'esposizione al pericolo, nel primo caso, può essere dovuta a una pluralità di fattori legati alla composizione fisica del prodotto, o alla relativa collocazione ambientale. Nella dimensione digitale, invece, la stessa è dovuta esclusivamente ad un uso improprio o un abuso delle informazioni: vuoi per tipologia di contenuti (dalla disinformazione, alla manipolazione, alla induzione a dipendenza o alla violenza, ai contenuti illeciti, discriminatori, o a sfondo sessuale), vuoi per l'accesso alle attività di trattamento (uso e riuso non autorizzati, furto di identità, etc).

Sotto il profilo della sicurezza, pertanto, la valutazione di impatto con le lenti dei diritti dell'infanzia consiste nell'effettuare una analisi circa l'adeguatezza delle misure tecnico-organizzative adottate dallo sviluppatore per un utente adulto, rispetto alle vulnerabilità del minore di età (e, dunque, *in primis*, la ridotta maturità in termini di capacità di discernimento), per poi declinare altri possibili profili, relativi alla maggiore o minore esposizione del singolo utente ad essere vittima di condotte improprie e abusive da parte di terzi. Il ruolo della valutazione di impatto relativa alla protezione dei dati si concretizza, pertanto, nell'identificare le misure più appropriate per garantire la disponibilità, l'integrità e la confidenzialità dei flussi, secondo un modello di *governance* ritenuto efficace a proteggere in quel particolare servizio o prodotto quegli utenti minori di età che ragionevolmente lo utilizzano. Diventa prioritario e preliminare, dunque, che i servizi e prodotti digitali possano attivare funzionalità specifiche laddove l'utenza sia composta (più o meno prevalentemente) da minori di età.

Funzionalità di c.d. *age-verification* costituiscono la prima misura che consentirebbe di attivare meccanismi di protezione per gli utenti non adulti che, come osservato nel capitolo precedente, potrebbero attuare in via automatica il regime per i dati cc.dd. sensibili in seno alla normativa nazionale. A tal fine, le tecniche presenti sul mercato sono molteplici e già in continua evoluzione. Per tale ragione, sono stati recentemente istituiti dei gruppi di lavoro volti a riconoscere dei percorsi di standardizzazione in modo da poter uniformare i requisiti tecnici e certificare il raggiungimento di obiettivi minimi di accuratezza,

precisione e dunque di affidabilità del meccanismo, anche utilizzando sistemi di IA. Ad esempio, il menzionato Istituto IEEE ha costituito un gruppo di lavoro per elaborare *standard* volti a identificare i requisiti tecnici per progettare, valutare e implementare sistemi di verifica dell'età in un determinato servizio della società dell'informazione. In particolare, l'analisi converge sull'identificazione di quattro livelli di affidabilità: *i)* asserito, *ii)* *standard*, *iii)* rafforzato e *iv)* rigoroso da poter certificare in base a determinati requisiti di riservatezza e sicurezza dei dati nel processo di verifica dell'età ⁽⁶¹⁾. L'International Organisation for Standards (ISO), invece, ha pubblicato un quadro di riferimento internazionale per i sistemi di verifica dell'età da utilizzare per ammettere o meno l'accesso a un prodotto, contenuto, o servizio (come la fornitura di liquori, tabacco, armi o contenuti *online*) da parte di un consumatore ⁽⁶²⁾. La norma distingue cinque livelli di affidabilità: rispetto alla proposta di IEEE si aggiunge dunque un livello minimo — chiamato “zero” (basato sulla mera dichiarazione senza validazioni) — e distingue un livello massimo, denominato “*strict*”, da un livello avanzato, c.d. “*enhanced*”, che si differenziano solo per gli ambiti di applicazione. La stessa norma ISO identifica anche una procedura di valutazione della conformità allo *standard* e di conseguente certificazione.

La Commissione Europea ha istituito una *task force* sulla verifica dell'età nell'ambito del Digital Services Act, in considerazione delle norme sulla protezione dei minori di età nelle piattaforme digitali che abbiamo commentato nel capitolo precedente, e in particolare della necessità che tali sistemi debbano poter operare senza richiedere dati ulteriori rispetto a quelli processati per aderire a un servizio, o attivare un prodotto ⁽⁶³⁾.

La prima riflessione che uno sviluppatore (o un produttore) di servizi digitali o di sistemi tecnologici deve effettuare è quella relativa alle misure tecniche e organizzative che siano necessarie (ma anche sufficienti) a definire l'utenza vulnerabile in quanto minore di età.

⁽⁶¹⁾ IEEE Standard for Online Age Verification, 2089.1-2024, https://standards.ieee.org/ieee/2089.1-2024_Cor_1/11923/.

⁽⁶²⁾ ISO/IEC JTC1/SC27/WG5, <https://euconsent.eu/download/iso-working-draft-age-assurance-systems-standard/>.

⁽⁶³⁾ EU Commission, *Digital Services Act: Task Force on Age Verification*, 2024, <https://digital-strategy.ec.europa.eu/en/news/digital-services-act-task-force-age-verification-0>.

La seconda, invece, deve concentrarsi sulla capacità del servizio o prodotto di proteggere l'utente minore di età all'esposizione ai rischi noti ⁽⁶⁴⁾. Su questa scia, al fine di tutelare l'utente dal fenomeno della disinformazione in senso ampio — che può concernere notizie non veritiere, manipolative, come le *fake news* ⁽⁶⁵⁾ — che mina l'autodeterminazione della persona, specialmente di un soggetto il cui pensiero è in formazione, ovvero proteggerlo da contenuti che possano indurlo a comportamenti violenti o che minaccino l'incolumità sua o di terzi — come in caso di *cyberbullismo*, discorsi d'odio o discriminatori ⁽⁶⁶⁾ — occorre procedere ad una analisi che combini la probabilità di occorrenza con la gravità e serietà delle minacce alla sicurezza e incolumità della persona.

Inoltre, laddove si percepisca un rischio minimo, ma continuo, di esposizione a contenuti impropri, occorre analizzare nel lungo termine le ricadute sul benessere di un organismo in crescita. Infatti, l'utente, anche in ragione di fattori socio-culturali e dell'ambiente in cui vive, può recepire una certa sollecitazione in maniera più o meno intensa. Le possibili ricadute comportamentali, educative, intellettuali ed emotive devono essere valutate, perciò, sia qualitativamente che quantitativamente, secondo una scala crescente di implicazioni negative sulla sfera personale dell'utente il cui sviluppo psicofisico è in formazione.

Le stesse possono infatti indurre a replicare un atteggiamento innocuo, ma improprio rispetto ai valori condivisi, oppure a prendere parte ad attività dannose per lo sviluppo dell'utente, in quanto inquietanti o non appropriati all'età, a emulare comportamenti pericolosi, attraverso sfide o giochi, come nel noto caso della *Blue Whale*, consistente nel proporre per un periodo una serie di compiti ad adolescenti depressi, aumentando di volta in volta il relativo livello di autolesionismo, fino a indurre i giocatori al suicidio, o altre simili come *Chroming* ⁽⁶⁷⁾ o il recentissimo *train surfing* ⁽⁶⁸⁾. Per gli ulteriori rischi che

⁽⁶⁴⁾ EU Commission, *EUKidsOnline survey*, IP/11/479. See previous remarks on the topic in the contribution: D. AMRAM, *Children (in the digital environment)*, in G. COMANDÉ (ed.), *Elgar Encyclopedia of Law and Data Science*, 2022, pp. 64 ss.; Council of Europe, *Challenges to Children's Rights Today: What Do Children Think?* (2015), Capitolo 8.

⁽⁶⁵⁾ E.C. TANDOC, Z.W. LIM AND R. LING, *Defining "fake news": A typology of scholarly definitions*, 2017, *Digital Journalism*, 6, 137 ss.

⁽⁶⁶⁾ S.C. VESTERGAARD (ed.) *Encyclopedia of Bullying*, Nova, 2020.

⁽⁶⁷⁾ Tali condotte sono contrarie anche all'art. 6 della CRC, si veda J.E. DOEK, *Article 6 CRC and the views of the CRC Committee*, 2015, 26 *Stellenbosch L. Rev.* 254.

minano la sfera intima e sessuale dell'utente, come le descritte condotte riconducibili al *grooming* o al *sexting* ⁽⁶⁹⁾, che possono sfociare in abusi da parte di utenti coetanei, oppure integrare illeciti penali laddove perpetrate da adulti, la necessità di identificare e mitigare il rischio di esposizione è senz'altro più urgente, in quanto agire *ex post* implica necessariamente il verificarsi di un pregiudizio serio e grave per l'utente minorenne.

L'elemento comune consiste nel fatto che l'esposizione ai pericoli sia determinata, in ogni caso, dall'elaborazione di dati, specialmente foto, immagini, video, ma anche testi ⁽⁷⁰⁾, che può avvenire sia attraverso *social network* o piattaforme, sia con servizi di messaggistica istantanea. Si tratta di operazioni di trattamento di dati, pertanto, dal punto di vista tecnico, le relative misure di salvaguardia riguardano la gestione di flussi di informazioni, affinché gli stessi siano disponibili secondo il livello di granularità compatibile con la protezione degli utenti minorenni, assicurando al contempo un livello di confidenzialità idoneo alla tipologia di informazione condivisa e un sistema di verifica rispetto a manipolazioni che possa ritenersi adeguato alla tipologia di utenza.

Con riferimento alle modalità di accesso e condivisione di contenuti da parte dell'utente, l'implementazione di interfacce che consentano una moderazione da parte del genitore può risultare efficace: ad esempio, certe funzionalità di applicativi di messaggistica istantanea possono essere predisposti, affinché immagini e video non siano né

F. LIAT - G. KHALID, *The criminalization of cyberbullying among children and youth*, 2019, 17 Santa Clara J Int'l L 1ff. Si vedano le misure adottate dal garante italiano contro la piattaforma Tik Tok a seguito del suicidio di una bambina di 10 anni <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9524224>; (2019), o dell'autorità garante olandese <https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-investigate-tiktok>, da ultimo si veda la decisione dell'EDPB, *Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited* (Art. 65 GDPR), https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_en.

⁽⁶⁸⁾ Open, *Diciottenne aggrappato su un treno per oltre 100 km*, <https://www.open.online/2024/07/10/train-surfing-18-enne-treno-regionale-ancona/>.

⁽⁶⁹⁾ Laboratorio Adolescenza e Istituto di Ricerca (LARD), *Indagine nazionale sugli stili di vita degli adolescenti che vivono in Italia*, edizione 2024, <https://laboratorioadolescenzamagazine.org/3018/>.

⁽⁷⁰⁾ B. KNOWLES, S. BECK, J. FINNEY, J. DEVINE AND J. LINDLEY, *A scenario-based methodology for exploring risks: Children and programmable IoT*, DIS'19 Proceedings (2019) 751 ss.

inviati, né scaricati dall'utente minorenne senza l'autorizzazione del genitore ⁽⁷¹⁾. Altre misure, invece, devono poter essere adottate a prescindere dal formato delle informazioni rese disponibili.

Il quadro si complica nel caso di trattamenti su sistemi disponibili ad utenti minori di età che si basano su tecniche di intelligenza artificiale. L'elaborazione dei dati, infatti, avviene attraverso un sistema decisionale automatizzato e solo da un progressivo monitoraggio dell'uso di un determinato applicativo si rendono evidenti possibili esposizioni a rischi e pericoli per l'incolumità psico-fisica dell'utente. In questo caso, lo sviluppatore deve poter declinare il requisito della supervisione umana della macchina tenendo conto delle vulnerabilità proprie dell'utilizzatore finale. Ad esempio, i giocattoli dotati di *chatbot* in grado di monitorare e registrare le abitudini, i comportamenti, le voci dei bambini, senza che i loro genitori, o adulti di riferimento, abbiano alcun controllo su tale tipo di trattamento dei dati o sui mezzi e sulle finalità di quelle poste in essere dopo la raccolta dei dati, espone i bambini agli stessi rischi rispetto a un conferimento diretto di informazioni. Infatti, da un lato, l'interazione col gioco potrebbe essere bersaglio di specifiche strategie pubblicitarie, incluso il *marketing* manipolativo e, dall'altro, usi anche imprevedibili, poiché nessuno ha il controllo su quel tipo di informazioni e tutele applicate ai flussi di dati prima di essere condivisi con terzi.

Con riferimento all'impatto sulla libera formazione del pensiero, invero, studi comportamentali ⁽⁷²⁾ hanno notato come — specialmente nell'età delicata dell'adolescenza — sistemi di *chatbot* catturino la fiducia del minore, che ne diviene più o meno rapidamente dipendente, per compiere qualsiasi tipo di scelta: ad esempio è emerso che dalla richiesta di conferme in ordine all'*outfit* da indossare in ragione delle previsioni meteorologiche, si sia passati repentinamente a chiedere conferma su una pluralità di elementi quotidiani che vanno ad incidere

(71) Come si evince dalle condizioni di utilizzo di alcuni smartphone (<https://support.apple.com/en-bh/105121>, https://play.google.com/store/apps/details?id=ua.com.tim_bern timers.parental_control&hl=en).

(72) N. KURIAN, (2024), 'No, Alexa, no!': *designing child-safe AI and protecting children from the risks of the 'empathy gap' in large language models*, in *Learning, Media and Technology*, 1-14. <https://doi.org/10.1080/17439884.2024.2367052>.

sull'autonomia della persona nelle scelte quotidiane, manipolando — di fatto — lo sviluppo dell'identità della persona ⁽⁷³⁾.

Dal lato pratico, si osserva che piattaforme di uso comune per i giovani, come TikTok, hanno recentemente adottato *policy* finalizzate a sottrarre i profili dei soggetti minori di età da pratiche commerciali dirette a monitorare l'utente bambino durante l'uso del servizio. Il che consente di ridurre notevolmente l'esposizione di soggetti la cui capacità di discernimento è limitata o non completamente sviluppata da pratiche manipolative volte a rendere l'utente un consumatore particolarmente incline a veicolare i propri comportamenti rispetto a forme di pubblicità e altri contenuti proposti con una limitata attitudine critica ⁽⁷⁴⁾.

Sotto il profilo dell'interazione persona-macchina e, nel nostro caso, bambini-macchina, la valutazione di impatto deve pertanto andare oltre la gestione dei flussi di dati e riguardare una sfera più complessa, quella dell'educazione — chiamata nel Regolamento sull'IA, come osservato, “*AI literacy*” — e del concetto di supervisione umana — *human oversight*. Dal lato pratico, si dovrebbero poter individuare i profili di criticità in fase di sviluppo e presentazione dei prototipi attraverso il coinvolgimento di rappresentanti della società civile che includano genitori, educatori, minori di età stessi e sviluppare campagne di conoscenza e sensibilizzazione nelle forme ritenute più efficaci (dal tutorial, alla *brochure*, al podcast e agli eventi), al fine di cogliere i possibili effetti distorsivi nell'uso della tecnologia, sviluppando raccomandazioni per un uso consapevole del servizio e prodotto ⁽⁷⁵⁾.

⁽⁷³⁾ H. ALEXA, S. CORTESI, A. LOMBANA-BERMEDEZ, AND U.GASSER, *Youth and Artificial Intelligence: Where We Stand*, 2019, Berkman Klein Center for Internet & Society publication.

⁽⁷⁴⁾ J. AUSLOOS, V. VERDOODT, *Confusing by design: A data protection law analysis of TikTok's privacy policy*. Report prepared for BEUC, 2021, https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-010_confusing_by_design-a_data_protection-law_analysis_of_tiktok_s_privacy_policy.pdf.

⁽⁷⁵⁾ Una ricerca commissionata da OfCom e ICO nel Regno Unito si è occupata di analizzare la percezione da parte di genitori e figli degli strumenti adottati dalle piattaforme per la verifica dell'età: in particolare, l'autodichiarazione, l'introduzione di identificatori, profilazione dei comportamenti, conferma del legale rappresentante, analisi del riconoscimento facciale, DIGITAL REGULATION COOPERATION FORUM, *Families' attitudes towards age assurance*, https://www.drcf.org.uk/__data/assets/pdf_file/0037/258688/Families-attitudes-towards-age-assurance.pdf.

Nei paragrafi precedenti sono emerse diverse indicazioni di politica del diritto volte a responsabilizzare il genitore e gli educatori a effettuare bilanciamenti caso per caso rispetto all'uso quotidiano della tecnologia da parte del minore. Abbiamo in particolare osservato come esigenze di protezione possano portare a regolamentare dei divieti di accesso a certi sistemi e applicativi, il che tuttavia mal si concilia con l'esigenza di formare cittadini — digitalizzati — consapevoli, nonché con i necessari contemperamenti derivanti dalla progressiva acquisizione di competenze e conoscenze che possono rendere l'adolescente un utente di prodotti e servizi della digitalizzazione sufficientemente autonomo. Atteggiamenti *by default* di proibizione dell'uso possono essere contemperati — da autorizzazioni da parte del genitore a spazi di autonomia e libertà commisurati alla maturità del minore di volta in volta accertata.

Il problema che si pone è quello relativo alla necessità di distribuire le responsabilità connesse all'accertamento della capacità di discernimento: da un lato, il genitore o l'educatore possono modulare le funzionalità di protezione in considerazione dell'autonomia del singolo minore di età; dall'altro lato, occorre che siano presenti possibili strumenti di segnalazione di pericoli, ovvero di condotte da parte dell'utente che possano essere nocive per se stesso e per terzi, in modo da consentire di ripristinare l'intervento dell'esercente le responsabilità genitoriali o dell'educatore.

Anche in questo caso, tuttavia, la valutazione di impatto resta attualmente una attività lasciata alla percezione dell'operatore economico, mentre il riconoscimento di *standard* tecnici consentirebbe una applicazione omogenea degli stessi. In termini di politica del diritto, un incentivo rivolto agli operatori ad adoperarsi affinché siano identificati strumenti per valutare in maniera oggettiva la capacità del minorenne ad agire come utente consapevole, soprattutto laddove abbia compiuto una certa soglia di età e dato prova di un certo livello di alfabetizzazione digitale, potrebbe nel lungo periodo soddisfare sia l'esigenza di assicurare una dimensione digitale più sicura, che quella di promuovere la partecipazione consapevole degli utenti più giovani.

Sul piano giuridico, occorrerebbe esplicitare il ruolo dell'adesione a *standard* tecnici come strumenti di misurazione della diligenza dei diversi attori che potrebbero essere chiamati a rispondere di pregiudizi occorsi ad utenti minorenni.

6. **Sviluppare un sistema di tutele nell'ordinamento italiano a partire dalle esperienze straniere.**

Dalla normativa europea emerge che l'attenzione ai minori di età sia prestata secondo due direttrici: la prima, quella formale, legata all'individuazione di soglie di età che possano far presumere la capacità di discernimento. La seconda, di responsabilizzazione degli utenti economici, attraverso l'imposizione di obblighi di *due diligence* e valutazione dei rischi propri della categoria di soggetti, rispettivamente per il titolare del trattamento, prestatore di servizi digitali, sviluppatore, fornitore, o distributore, o *deployer* di soluzioni basate sull'IA finalizzati alla implementazione caso per caso di misure tecnico-organizzative necessarie per la relativa mitigazione.

Le normative sulla regolamentazione della società dell'informazione o dell'innovazione tecnologica non aggiungono ulteriori profili per i minori di età, salvo quelle che inquadrano sotto il regime dei dati sensibili le informazioni concernenti i bambini, abilitando una serie di tutele legate alle specifiche basi di giuridiche dei trattamenti.

Abbiamo osservato, poi, come alcuni sistemi abbiano adottato delle iniziative *ad hoc*, andando a inquadrare la tutela dei diritti digitali dei minori alla stregua di una normativa di settore. Per alcune, come l'OSA o le iniziative degli stati americani o cinese si tratta di elevare a rango di fonte primaria obblighi e procedure a carico di organizzazioni o degli adulti di riferimento (genitori, esercenti le responsabilità genitoriali, educatori, etc.). L'unica legislazione che comprenda principi, diritti e modalità di attuazione è quella brasiliana che attribuisce efficacia normativa al riconoscimento della dimensione digitale dei diritti del fanciullo già oggetto di regolamentazione nello statuto dell'infanzia e dell'adolescenza, e individua anche diritti propri della dimensione digitale.

In Europa, invece, salvo per alcune funzionalità e filtri "*a misura di bambino*" offerte direttamente nell'ambito dei termini e condizioni d'uso di servizi o prodotti della società dell'informazione, che permettono al genitore di intervenire sulle impostazioni dei profili di accesso, non sussiste alcuna norma che veicoli l'intermediazione con i genitori, rendendola obbligatoria.

Come osservato, infatti, sia il GDPR che il DSA, letti in combinato disposto, impongono di effettuare una valutazione di impatto ritagliata alle esigenze degli utenti minori di età, senza introdurre normativamente alcuna interlocuzione tra prestatori di servizi e genitori/legali

rappresentanti per il controllo e monitoraggio delle attività dell'utente minorenni. Il coinvolgimento del genitore, infatti, diventa una misura di mitigazione del rischio valutato dal titolare del trattamento/prestatore di servizio digitale, che si traduce — al più — in una clausola, di tipo contrattuale, per l'accesso ai servizi o l'utilizzo dei prodotti e il relativo mantenimento. Di conseguenza, chiunque potrebbe creare profili correttamente registrati a nome dell'adulto e fruire del servizio digitale attivato in nome e per conto di quest'ultimo con filtri e misure di salvaguardia introdotti a discrezione dell'utilizzatore.

Questa prospettiva assume particolare rilevanza in termini di ricadute di sistema, in quanto la mancata previsione di un intervento proattivo del genitore nella configurazione delle modalità di accesso e uso dei servizi della società dell'informazione demanda necessariamente al generale obbligo di cura genitoriale.

Ciò porta, anche in ragione delle possibili diverse sensibilità emergenti dal contesto sociale in un determinato momento storico, anche a percepire i rischi e, pertanto, a configurare una pluralità di modelli educativi. Gli stessi potrebbero, tuttavia, essere messi in discussione solo in caso di scenario patologico in cui uno dei rischi percepiti per il minore — quale utente digitale — effettivamente si verifichi, al fine di accertare una possibile responsabilità da omessa cura o protezione. Peraltro, in caso di possibile divergenza di opinione tra i due genitori o, addirittura, tra genitori e figlio adolescente, può insorgere una situazione conflittuale, da mediare o risolvere fuori dalle mura domestiche: in tali casi è demandando al giudice o al mediatore il compito di interpretare quale sia la soluzione che meglio persegua il c.d. *best interest of the child*.

In assenza di specifici obblighi per i genitori di porre in essere condotte di protezione, il paradigma che emerge dal sistema di tutele delle vulnerabilità della prole nell'ambiente digitale appare essere quello tradizionale della responsabilità genitoriale. A questo proposito, occorre investigare in che termini il meccanismo della responsabilizzazione adottato per gli operatori dalla strategia europea dei dati, possa emergere da una interpretazione sistematica delle fonti rilevanti.

La responsabilizzazione appare riversarsi sulle organizzazioni, pubbliche o private, attraverso l'incentivazione di interventi virtuosi volti a sensibilizzare la società civile, rendendo utenti consapevoli non solo i giovani, ma anche (e soprattutto) agli adulti, per consentire loro di poter prendere decisioni appropriate nell'esercizio delle relative responsabilità di cura e protezione, sia in termini di sicurezza, che in

ottica di monitoraggio rispetto allo sviluppo di forme di dipendenza. Questo sistema, tuttavia, non appare completamente soddisfacente nel breve periodo, in quanto mancherebbero oggi strumenti di attuazione specifici per responsabilizzare l'azione individuale verso gli obiettivi di prevenzione e mitigazione dei rischi specifici della digitalizzazione di una pluralità di attività quotidiane della vita dei bambini.

6.1. (Segue). *Le responsabilità genitoriali nella dimensione digitale.*

La riflessione sulla protezione e promozione dei diritti dei minori nella dimensione digitale nel nostro sistema richiede una duplice verifica: da un lato, comprendere se le misure di attuazione delle iniziative legislative in materia di strategia dei dati e innovazione introducano disposizioni *ad hoc* sui soggetti vulnerabili e, in particolare, per i minori di età; dall'altro lato, analizzare le novità legislative con gli istituti esistenti per valutare eventuali tensioni e interpretazioni sistematiche per garantire la tenuta di sistema.

A questo proposito, abbiamo osservato nel primo capitolo e analizzato nei paragrafi precedenti come il dato formale del compimento di una certa età possa costituire da abilitatore di flussi di informazioni personali per i servizi della società dell'informazione. L'introduzione di una soglia diversa dal compimento della maggiore età necessita, tuttavia, di accomodamenti ragionevoli in sede di interpretazione per superare le criticità in ordine al disallineamento tra capacità di prestare un consenso valido a fini di trattamento dei dati personali e capacità di compiere atti negoziali per l'adesione a un servizio digitale.

A completamento della riflessione, appare utile analizzare cosa accada in caso di illecito, al fine di comprendere se l'autonomia accordata per esprimere il consenso nella società dell'informazione possa avere ricadute in caso di patologia dei rapporti tra privati o se debbano comunque innescarsi quei meccanismi di allocazione di responsabilità in capo ai genitori.

Nella dimensione digitale il prestatore di servizi o prodotti digitali è tenuto a proteggere i minori di età sulla base del quadro di riferimento ricostruito incidendo su profili di tipo soprattutto tecnico e di gestione dei flussi di dati. L'approccio ha delle implicazioni evidenti sul ruolo dei genitori (legali rappresentanti) nei processi educativi dei figli e, di conseguenza, sull'esercizio delle relative responsabilità.

Con riferimento a condotte attive nella dimensione digitale da parte del genitore, nulla sembra cambiare rispetto a quella fisica: il paradigma di responsabilità intrafamiliare trova, infatti, applicazione laddove il genitore leda un diritto fondamentale del proprio figlio attraverso condotte attive o passive: la giurisprudenza di merito, ad esempio, ha avuto modo di concentrarsi già da qualche anno sulla declinazione dell'interesse superiore del minore a fronte della condivisione di informazioni relative alla vita privata o di immagini relative ai figli da parte dei genitori, specialmente in scenari conflittuali tra genitore-figlio adolescente, o tra genitori separati. In questi casi, in maniera pressoché unanime, i tribunali hanno adottato un atteggiamento restrittivo per cui — visti i rischi noti e considerata l'impossibilità di prevedere implicazioni in futuro della condivisione di informazioni o immagini riguardanti minori di età su piattaforme digitali — in assenza di un consenso tra i due rappresentanti legali, ovvero in presenza di una manifestazione di dissenso da parte del minore, ritenuto capace di esprimere consapevolmente la propria opinione in proposito, la condotta cc.dd. di *sharenting* è stata inibita, talvolta anche mediante la comminazione di *astreinte* ⁽⁷⁶⁾ e i conseguenti pregiudizi risarciti ⁽⁷⁷⁾.

Altre condotte che rilevano in termini di illecito civile intrafamiliare possono riguardare il mancato esercizio del diritto di visita se accordato telematicamente ⁽⁷⁸⁾.

Ci si può domandare se, in ragione delle esigenze di sviluppare abilità digitali e vista l'attenzione del legislatore europeo alla alfabetizzazione si possa rinvenire — nell'ambito del dovere di educare e istruire i figli — una possibile mancanza riguardante le abilità informatiche e tecnologiche, laddove si fornisca l'accesso agli strumenti digitali.

La questione appare particolarmente interessante per tracciare nuovi confini in materia di responsabilità da *culpa in vigilando ex art.*

⁽⁷⁶⁾ *Ex multis*, Trib. Mantova, 19 settembre 2017, in *Fam. Dir.*, 2018, p. 380 con nota di NITTI, in *Resp. civ. prev.*, 2018, con nota di PIERON; Trib. Ravenna, 15 ottobre 2019, n. 1038, *inedita*.

⁽⁷⁷⁾ *Ibidem*.

⁽⁷⁸⁾ Cass. 6 marzo 2020, n. 6471, che indica l'incoercibilità del diritto di visita in termini di condanna di un *facere* in quanto estrinsecazione della relazione genitore figlio e, pertanto, del principio di autodeterminazione, in *Diritto Mercato e Tecnologia*, 2020, con nota di F. PIROZZI.

2048 c.c., sebbene oggetto di scarsa applicazione per il momento ⁽⁷⁹⁾. Purtuttavia, laddove si sdogani la circostanza che il minore adolescente possa assumere la posizione di utente consapevole *online*, diventa coerente verificare se e in che misura la responsabilità oggettiva dei genitori sia da circoscrivere.

In particolare, occorre riflettere se le condotte dell'adolescente che abbia compiuto gli anni previsti *ex art.* 8 GDPR e applicazione nazionale (nella specie dall'art. 2 *quinquies* del Codice in materia di protezione dei dati personali) ⁽⁸⁰⁾ possano produrre i medesimi effetti dell'“emancipazione”, rispetto all'ambito di applicazione dell'art. 2048 c.c. Ciò al fine di responsabilizzare l'utente minorenni e temperare la maggiore autonomia nella dimensione digitale con una ridotta garanzia — patrimoniale — da parte dei genitori.

Per emancipazione, infatti, si intende quell'istituto giuridico di rada applicazione oggi, legato per lo più alle esigenze di consentire al minorenni di esprimere consenso valido a contrarre matrimonio (emancipazione c.d. di diritto), ovvero di compiere da solo atti che non eccedono l'ordinaria amministrazione e, con l'assistenza del curatore, di riscuotere capitali sotto la condizione di idoneo impiego, di stare in giudizio (come attore o convenuto), di esercitare attività di impresa anche autonomamente, se autorizzato dal giudice tutelare ⁽⁸¹⁾. Appare tuttavia difficoltoso legare l'istituto allo scenario relativo alla navigazione *online* o all'uso di prodotti tecnologici.

Verosimilmente, anche nelle circostanze dell'adesione a un servizio o prodotto della società dell'informazione, è la capacità di discerni-

⁽⁷⁹⁾ Trib. Caltanissetta, 8 settembre 2019 incarica il Servizio sociale di monitorare e supportare il genitore ad educare il figlio al rispetto dei coetanei nei servizi di messaggistica istantanea. La decisione cita un precedente del Trib. Teramo, 16 gennaio 2012, che invece affronta la questione legata alla responsabilità dei genitori *ex art.* 2048 c.c. per danno cagionato attraverso *social network* e specifica che “il dovere di vigilanza dei genitori deve sostanzialmente in una limitazione sia quantitativa che qualitativa di quell'accesso, al fine di evitare che quel potente mezzo fortemente relazionale e divulgativo possa essere utilizzato in modo non adeguato da parte dei minori” in *Diritto e giustizia*, 2020, <https://www.dirittoegustizia.it/#/documentDetail/9204218>.

⁽⁸⁰⁾ Art. 2 *quinquies*, d.lgs. n. 196 del 2003, così come modificato da d.lgs. n. 101/2018, prevedendo che il minore che abbia compiuto quattordici anni possa esprimere in Italia consenso valido per il trattamento dei dati in relazione all'offerta diretta di servizi della società dell'informazione.

⁽⁸¹⁾ L'emancipazione, in caso di matrimonio, è condizione prevista dall'art. 390 c.c. in combinato di sposto con l'art. 84 c.c., mentre è oggetto di richiesta autonoma laddove lo scopo esuli dal matrimonio.

mento legata alla crescente autodeterminazione del minore ad apparire presuntivamente adeguata, già prima del compimento del diciottesimo anno di età ⁽⁸²⁾.

In questa prospettiva, pertanto, appare preferibile poter verificare se sia possibile limitare la responsabilità del genitore attraverso la prova liberatoria di cui all'art. 2048 c.c., ultimo comma, consistente nel “*non aver potuto impedire il fatto*”. In effetti, a fondamento della responsabilità oggettiva per i genitori vi è la colpa collegata all'omessa vigilanza. In un sistema che autorizza il minorenni a divenire utente, appare difficile escluderne la responsabilità per le condotte compiute. A questo proposito, però, appare necessario comprendere che ruolo possa avere l'eventuale incapacienza del patrimonio del minore a fini risarcitori della vittima di un uso illecito dei servizi o dei prodotti digitali.

Se si esclude l'applicabilità di cui all'art. 2048 c.c., sembra difficile poter giustificare un meccanismo di responsabilità solidale, salvo che si introduca una norma simile all'art. 2054 c.c. ⁽⁸³⁾ in materia di circolazione dei veicoli, che, a fini di maggior tutela della vittima, individui una sorta di garante (*rectius* responsabile in solido) del soggetto verosimilmente più capiente a rispondere patrimonialmente dei danni arrecati, sulla scia di quanto avviene tra conducente e proprietario del mezzo. Tra le figure co-responsabili vi potrebbe essere, in prospettiva, oltre al genitore, il titolare della specifica utenza, relativa alla linea dati del minorenni.

Mentre il primo costituirebbe un garante “naturale” della posizione del minore di età, il secondo — non necessariamente coincidente con il legale rappresentante — potrebbe assumere una tale responsabilità solo laddove vi sia un effettivo controllo sull'utenza (escludendo dunque possibili doni) e laddove ci sia un meccanismo di certificazione delle capacità dell'utente-minorenni, alla stregua della patente di guida per i ciclomotori.

In altri termini, al fine di poter allineare il sistema di responsabilità civile a logiche di risarcimento integrale e allo stesso tempo accrescere il livello di educazione digitale, potrebbe, in prospettiva di *de iure*

⁽⁸²⁾ B. AGOSTINELLI, “*Emancipazione digitale*” e tutela dei minori tra responsabilità genitoriale e regolamentazione eurounitaria, in R. TORINO e S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023 p. 179 ss.

⁽⁸³⁾ S. POLLASTRELLI, *Circolazione di veicoli*, Comm. già P. Schlesinger, Busnelli Ponzanelli, Giuffrè, 2022.

condendo, individuarsi un meccanismo di certificazione, quale condizione per poter attivare, da un lato, premi assicurativi o scenari di limitazione delle responsabilità per fatto del terzo e, dall'altro lato, rendere più sicuro l'ambiente digitale attraverso una effettiva assimilazione armonizzata delle regole di fruizione di servizi e prodotti, che saranno così recepite e attuate su larga scala.

6.2. (Segue). *Verso un patentino per l'utente minorenne?*

Prende forma così la possibilità di identificare programmi di rafforzamento delle competenze comuni al livello (almeno) di Unione Europea, ma estensibile anche a paesi terzi, attraverso ad esempio previsioni *ad hoc* in codici di condotta dei prestatori di servizi o produttori ⁽⁸⁴⁾.

Considerando i dati sulle esposizioni e navigazioni *online* ⁽⁸⁵⁾, occorre che la scelta dell'età minima per accedere al percorso possa non solo essere legata al valore più basso della forbice prevista dal GDPR, ma anche consentire una formazione con valutazione per i bambini che, ad esempio, frequentino la scuola primaria di secondo grado. Infatti, se statisticamente un terzo degli utenti *online* ha un'età compresa tra gli anni 11 e gli anni 16, iniziative di armonizzazione delle competenze finalizzate ad una navigazione, seppur limitata, in generale più sicura, devono poter guardare oltre il limite previsto per il trattamento del dato personale nella società dell'informazione.

Il paragone con il sistema della patente di guida, infatti, era già stato oggetto di iniziative europee per la creazione di competenze sull'uso di *software*, nella c.d. ECDL, patente europea del computer, volta a rendere i giovani adulti più competitivi rispetto all'uso di strumenti informatici ⁽⁸⁶⁾. Più di recente, il programma DigComp della Commissione Europea stila le aree di competenza e le conoscenze da

⁽⁸⁴⁾ H. GREIJN, V. HAUCK, A. LAND, J. UBELS, *Capacity Development & Technical Cooperation: Capacity Development Beyond Aid*, May 2015; United Nations Development Programme (UNDP), *Capacity Development: A UNDP Primer*, 2009.

⁽⁸⁵⁾ UNICEF, *The State of the World's Children 2017: Children in a digital world*, cit.

⁽⁸⁶⁾ European Computer Driving Licence, oggi Certificazione Internazionale di Alfabetizzazione Digitale (International Certification of Digital Literacy, ICDL), <https://www.icdl.it/>.

acquisire per otto livelli al fine di formare cittadini digitalmente consapevoli ⁽⁸⁷⁾.

Orbene, al pari della predetta esperienza, la proposta di “*patentino digitale*” muove dalla duplice necessità di creare conoscenze e competenze per un ambiente digitale più sicuro e a portata di bambini.

Sulla base del livello di abilità certificate, infatti, potrebbero essere attivate alcune funzionalità, altrimenti non accessibili all'utente. In questo modo, il dato formale dell'età anagrafica verrebbe normalizzato all'effettiva valutazione della consapevolezza, utile quanto meno a fini di *due diligence* e *accountability* per gli operatori economici.

Il fatto di introdurre nei termini e condizioni d'uso la necessità che l'utente sia “*patentato*”, faciliterebbe al prestatore di servizi o di prodotti digitali la possibilità di fornire la prova di aver verificato l'età e il livello di *literacy* dell'utente. Resterebbe la necessità di attribuire eventualmente a ciascun livello di certificazione un accesso a servizi o funzionalità diversificate in ragione della valutazione del rischio.

Per le istituzioni, la creazione di un “patentino” costituirebbe un meccanismo per incentivare il cambiamento culturale delle generazioni correnti e un mezzo per promuovere un ambiente digitale più sicuro.

Alle famiglie, a fronte di una formazione specifica, resterebbe così il compito di assicurarsi nel caso concreto — giorno per giorno — l'idoneità del minore a “navigare” tra i servizi e prodotti digitali, stabilendo regole per l'utilizzo dei sistemi informativi, applicando *mutatis mutandis* lo stesso metro che vale per consentire al figlio con patentino di guidare il ciclomotore. Per gli utenti minorenni, l'istituzione di un sistema di certificazione obbligatoria permetterebbe di ricevere una formazione specifica sui rischi ed opportunità della dimensione digitale, imparando — al pari del codice della strada — le regole da applicare per la sicurezza propria e degli altri.

7. Dalla protezione alla promozione dei diritti fondamentali nella dimensione digitale (*cenni e rinvio*).

In questo capitolo abbiamo esplorato le strategie normative, di

⁽⁸⁷⁾ R. VUORIKARI, S. KLUZER, Y. PUNIE, DigComp 2.2: *The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48883-5, doi:10.2760/490274, JRC128415.

diverso rango, per proteggere i minori dall'esposizione a pericoli nella dimensione digitale.

Dall'analisi emergono due profili particolarmente interessanti rispetto alle premesse della presente trattazione: il primo riguarda il fatto che le vulnerabilità dei minori di età derivano prevalentemente da una ridotta capacità di discernimento e, dunque, di prontezza a evitare di incorrere in scenari pregiudizievoli e per questo profilo, ciascun attore — istituzionale o privato, o persona fisica — è chiamato a tenere determinati comportamenti “*responsabili*” in ragione degli obblighi previsti dalle diverse iniziative legislative. Se, da un lato, operano, in questo caso, i normali meccanismi di responsabilità (declinabili in termini di *responsibility* introdotta *ex lege*, *liability* accertata giudizialmente in concreto in ipotesi di danno, e *accountability* in ragione della distribuzione di ruoli e responsabilità rispetto ad obblighi di valutazione di impatto, ad esempio, per gli operatori economici) ⁽⁸⁸⁾; dall'altro lato, il dato formale dell'aver compiuto o meno una certa età è condizione necessaria per applicare un determinato regime, ma non sufficiente ad escludere la sussistenza di uno stato di vulnerabilità rispetto ai pericoli oggetto di attenzione nella prospettiva di proteggere i minori di età. In altri termini, fenomeni di cyberbullismo, disinformazione, *grooming* etc. occorrono anche per l'utente adulto, ma non appare necessario dover intervenire con una tutela specifica in quanto la persona adulta dovrebbe poter essere in grado di prevenire e gestire gli effetti di possibili condotte senza che possa crearsi un nocumento per la propria persona, incolumità, salute, etc. Laddove le condotte illecite *per se* costituiscano anche un illecito penale — a prescindere dall'età della persona offesa — *nulla quaestio*, ma nelle situazioni in cui l'utente diventa vittima di un uso improprio della tecnologia da parte di terzi o di se stessi (si pensi allo sviluppo di dipendenze o alla disinformazione), essa resta vulnerabile anche se adulto, sia come singolo, che come appartenente ad un determinato gruppo.

La vulnerabilità per i bambini è presunta rispetto al profilo dell'autonomia e capacità di discernimento e in parte può essere superata attraverso azioni educative e di sensibilizzazione, come quella proposta di rafforzare gli strumenti di alfabetizzazione, sviluppo di competenze e conoscenze specifiche, proposte nel c.d. “patentino”. La stessa vul-

⁽⁸⁸⁾ Sia concesso rinviare al paradigma di responsabilità disegnato nelle relazioni familiari nel contributo D. AMRAM, *In familia respondere. La famiglia alla prova della solidarietà e del principio di responsabilizzazione*, Torino, 2020.

nerabilità resta in termini di esposizione a certi pericoli in ragione dell'asimmetria informativa, nonostante i possibili sforzi in termini di trasparenza che le normative impongono ai fornitori, sviluppatori, prestatori di soluzioni tecnologiche e digitali.

Il secondo profilo, invece, riguarda la transizione digitale delle vulnerabilità già note nella dimensione fisica e che richiedono una educazione digitale per evitare di incorrere in scenari pregiudizievoli, ma che allo stesso tempo sono forieri di possibili opportunità che consentirebbero — se colte — di arricchire di altrettanto nuovi contenuti la formula dell'interesse superiore del fanciullo e del perseguimento del relativo benessere.

Nel prossimo capitolo ci occuperemo di verificare le condizioni per promuovere il benessere di tutti i bambini e di tutti gli adolescenti nello spazio digitale.

CAPITOLO III

DIRITTI UNIVERSALI E VULNERABILITÀ MULTIPLE: PROMUOVERE IL BENESSERE DI TUTTI I MINORI DI ETÀ NELLA DIMENSIONE DIGITALE

SOMMARIO: 1. Diversità, inclusione e il diritto all'accesso alle risorse. — 1.1. (*Segue*). Le vulnerabilità multiple... — 1.1.1. (*Segue*). ...il settore educativo. — 1.1.2. (*Segue*). ...il settore sanitario. — 2. Muoversi attorno al piano dell'autonomia e della consapevolezza del singolo: il ruolo della trasparenza. — 3. L'educazione digitale: rafforzare conoscenze e competenze tecnologiche. — 4. Nuove tecnologie, gioco e creatività. — 5. Promuovere la sfera relazionale e quella emotiva. — 6. L'identità digitale e il problema della costruzione della reputazione. — 7. La prospettiva partecipativa nella dimensione digitale. — 8. La responsabilizzazione delle istituzioni e degli operatori economici. — 8.1. (*Segue*). La responsabilizzazione degli adulti e delle comunità di riferimento per il minore. — 9. Costruire una dimensione digitale assieme a (e alla portata di) bambini e adolescenti... — 9.1. (*Segue*). ...e le considerazioni di sistema. — 9.2. La declinazione dei cc.dd. *best interests of the child* e gli spazi di "adattamento". — 9.2.1. L'approccio anagrafico e orientato alla trasparenza. — 9.2.2. L'approccio a partecipazione consapevole e personalizzata. — 9.2.3. La combinazione dei due approcci.

Costruire un ambiente digitale e un ecosistema per l'innovazione a misura di bambini significa adoperarsi affinché i diritti nella dimensione digitale abbiano una portata universale: i principi di inclusività e non discriminazione devono poter, infatti, trovare attuazione nell'ambito dei meccanismi di tutela e promozione dell'utente vulnerabile.

Nelle pagine che seguono declineremo la formula dell'interesse superiore del fanciullo nell'ambito di scenari di vita comune ove i bambini e gli adolescenti realizzano la propria personalità non solo in quanto utenti della società dell'informazione o delle nuove tecnologie minori di età, ma come persone, eventualmente portatrici di ulteriori vulnerabilità, che contribuiscono alla datificazione della società con un ruolo attivo.

Osserveremo, infatti, l'articolarsi delle misure di salvaguardia e degli strumenti per il perseguimento dei migliori interessi in casi in cui

il bambino possa essere esposto a pericoli diversi, o di intensità maggiore, rispetto al modello astratto “dell’utente minorenni medio” cui paiono far riferimento le iniziative legislative e le prassi illustrate nel corso della trattazione. In particolare, proveremo a sviluppare possibili scenari in cui la capacità di discernimento sia ulteriormente ridotta da (o la riduzione sia accompagnata a) fattori distinti dalla immaturità dovuta allo sviluppo psico-fisico, del tutto comuni nella realtà.

Noteremo, infine, come molte delle vulnerabilità siano mitigabili con specifiche azioni formative che sviluppino una cultura di responsabilizzazione verso un ecosistema dei dati e delle tecnologie affidabile e sicuro. Forniremo, infine, raccomandazioni per raggiungere l’obiettivo di costruire spazi digitali a misura di bambino attraverso azioni e iniziative che siano frutto di una cooperazione multilivello promossa, da un lato, da obblighi di responsabilizzazione di operatori economici e, dall’altro, dai già esistenti sistemi di responsabilità e protezione per i soggetti deboli della società (non solo dell’informazione).

1. Diversità, inclusione e il diritto all’accesso alle risorse.

Promuovere i valori dell’UE nello spazio digitale significa garantire la parità di trattamento nell’accesso a prodotti e servizi del mercato unico: in attuazione del principio di non discriminazione, le iniziative dell’Unione muovono dalla necessità di assicurare che le diversità siano valorizzate per il contributo che le stesse possono offrire alla costruzione di una società più inclusiva e, dunque, più competitiva rispetto ai mercati extra europei ⁽¹⁾.

In questo quadro, la transizione digitale dei servizi e dei prodotti consente, da un lato, di abbattere barriere fisiche e geografiche, facilitando l’integrazione per quelle persone che altrimenti sarebbero escluse dalla fruizione di beni, servizi e capitali; mentre, dall’altro, la datificazione rende come indispensabile la possibilità di fruire dell’accesso alle risorse della società dell’informazione ⁽²⁾. Si tratta di infrastrutture, la cui presenza e capacità in termini di potenza costituisce un

⁽¹⁾ European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, COM(2010) 573 final, 19.10.2010.

⁽²⁾ European Commission, *European Data Strategy*, COM(2020) 66 final, 19.02.2020.

elemento abilitatore e, al contrario, la relativa assenza diventa una barriera culturale, sociale ed economica difficilmente superabile con mezzi propri dall'individuo. Anche le risorse culturali assumono un ruolo di grande impatto, considerata la necessità di rafforzare le conoscenze e le competenze dei diversi attori, affinché possano essere in grado di attivare e coltivare le opportunità della digitalizzazione.

L'accesso a un ambiente digitale sicuro e l'utilizzo di tecnologie affidabili costituiscono dei mezzi di raggiungimento di *standard* di inclusività che non trova precedenti nella storia ⁽³⁾. Conoscenze, esperienze e opportunità di crescita sono alla portata di tutti, a prescindere dal luogo geografico di connessione, dalla lingua parlata, dalla razza o etnia rappresentata, dal credo religioso, dallo stato di salute o dalla condizione socio-economica del nucleo familiare. L'abbattimento delle barriere fisiche permette, almeno in teoria, di raggiungere bambini che altrimenti non avrebbero alcuna possibilità di confronto su temi, risorse e persone.

Nei capitoli precedenti ci siamo sempre riferiti ai minori di età considerando in maniera astratta soggetti che non abbiano compiuto gli anni diciotto e utenti di servizi e prodotti della digitalizzazione, proceduralizzando le attività di valutazione e mitigazione di rischi genericamente applicabili a tutti gli appartenenti alla categoria.

Orbene, diversità e inclusione sono due principi che nello sviluppo di nuove tecnologie pongono una serie di quesiti tecnici ed etico-giuridici per qualsiasi categoria di utenti, a prescindere dall'età e dall'autonomia effettiva ⁽⁴⁾.

Perseguire gli interessi superiori dei bambini nella dimensione digitale significa cogliere quei fattori che consentano di raggiungere il più ampio grado di inclusività, promuovendo le diversità, adattando le considerazioni emergenti circa l'attuazione di misure antidiscriminato-

⁽³⁾ Si vedano i contributi contenuti nel volume G. FINOCCHIARO, L. BALESTRA, M. TIMOTEO (a cura di), *Major Legal Trends in the Digital Economy. The Approach of the EU, the US and China*, Bologna, 2022.

⁽⁴⁾ Le linee guida per una intelligenza artificiale affidabile, ad esempio, dedicano il quinto requisito a questi profili per garantire la parità di trattamento e di accesso alle soluzioni basate sull'IA. Il fatto che i processi decisionali siano automatizzati, infatti, richiede una attenzione a che la realtà sia rappresentata in maniera quanto più completa possibile. A tal fine, nel ciclo di vita dello sviluppo degli applicativi occorre introdurre procedure che consentano una verifica delle basi di dati da processare, dei risultati dell'elaborazione, attraverso una pluralità di attori che rappresentino idealmente tutte le parti interessate: ALTAI Checklist, *cit.*

rie valide per gli adulti, agli scenari di pericolo cui i bambini sono maggiormente esposti.

Prende forma il concetto di “vulnerabilità multiple” ⁽⁵⁾ da interpretarsi come possibili accomodamenti ⁽⁶⁾ che ragionevolmente l'operatore economico, ma più in generale la società civile, deve implementare per non escludere in maniera ingiustificata certuni e, allo stesso tempo, includere quante più rappresentazioni possibili della varietà umana, in quanto l'abbattimento delle barriere fisiche richiede una più profonda riflessione sulle possibili implicazioni universali nello spazio digitale ⁽⁷⁾.

In quest'ottica, il ruolo delle istituzioni è senz'altro quello di garantire, in primo luogo, l'accessibilità a risorse, purché sicure e affidabili. In secondo luogo, occorre prendere contezza delle ricadute pratiche sullo sviluppo cognitivo, linguistico e socio-emozionale di un uso quotidiano delle tecnologie e dei servizi digitali per ripensare il ruolo dei minori di età nei processi decisionali.

A questo proposito, in ragione della pericolosità insita nell'ambiente digitale, il fatto di sollecitare l'utente minorenni ad un comportamento responsabile e proattivo, unito all'acquisizione di nuove competenze e conoscenze, porta a dover esplorare nuove declinazioni del concetto di benessere del bambino utente delle nuove tecnologie, fermo restando il sistema multilivello di responsabilità descritto nel capitolo precedente. L'applicazione del principio di interesse superiore del fanciullo non può essere limitato a preservare e proteggere dai rischi e pericoli, ma deve necessariamente andare oltre e vagliare le possibilità per un miglior sfruttamento della tecnologia, in ragione della capacità di ciascuno di trarne il massimo beneficio, sia nella prospettiva di superare le frontiere della conoscenza e arricchire la persona di nuove abilità per meglio interpretare la società presente e il futuro, sia nell'ottica di superare gli ostacoli rispetto al raggiungimento di pari opportunità, per coloro che sono portatori, anche momentaneamente, di vulnerabilità tali da discostarsi dal parametro astratto percepito nelle

⁽⁵⁾ M. IENCA, *cit.*

⁽⁶⁾ G. COMANDÉ, *cit.*

⁽⁷⁾ Si pensi agli strumenti di applicazione sanitaria allenati con basi di dati esclusivamente di una determinata area geografica: l'accuratezza del processo decisionale deve essere ponderato con i limiti rispetto all'inclusività per cui lo strumento potrebbe non solo non funzionare, ma anche dare esiti impropri, con conseguenze pregiudizievoli, se utilizzato da / rispetto a un'utenza con caratteristiche genetiche o somatiche o fisiologiche diverse.

valutazioni di impatto, che potrebbe essere riassunto con “*utente minorenne medio*” (8).

Quest’ultimo profilo riguarda soprattutto le categorie più deboli: parità di accesso alle risorse della società dell’informazione non significa soltanto che le istituzioni debbano impegnarsi a mettere a disposizione strumenti tecnologici, ma anche promuovere iniziative, affinché l’utente bambino possa instaurare un rapporto diretto con soluzioni digitali e tecnologiche che gli garantiscano di acquisire competenze e conoscenze per affrontare il mondo reale, raggiungendo quotidianamente maggior grado di autonomia.

Se l’obiettivo è quello di costruire una società inclusiva, queste opportunità non possono essere concepite come un privilegio di alcuni, ma rappresentare un livello essenziale per la comunità. Con la conseguenza che, nell’interpretare l’interesse superiore del minore di età, sarà necessario effettuare un bilanciamento tra l’atteggiamento difensivo e quello propositivo. Tale bilanciamento darà priorità alle opportunità, laddove l’ambiente digitale raggiunga il livello di sicurezza che possa essere riconosciuto come *standard* in termini di misure tecnico-organizzative implementate e un livello di conoscenza e consapevolezza accettabile da parte dell’utente.

1.1. (Segue). *Le vulnerabilità multiple...*

Nella società dell’informazione affrontare le vulnerabilità multiple appare un’operazione paradossalmente più semplice, almeno per alcune di esse, da un punto di vista metodologico, rispetto alla realtà “analogica”, ove certe barriere devono essere superate fisicamente. Infatti, almeno con riferimento a quelle attività legate al trattamento di dati personali, le vulnerabilità sono rappresentate dalla natura e dalle proprietà dell’informazione.

(8) G. MALGIERI, *The notion of the data subject: an average individual?*, in *Vulnerability and Data Protection Law*, cit., Chapter 2, p. 17 ss. <https://doi.org/10.1093/oso/9780192870339.003.0002>. In un rapporto del JRC, si osserva che “*Research and development of AI systems for children are often carried out in the context of WEIRD (Western, Educated, Industrialised, Rich and Democratic) societies, and we need to make sure that technologies, methodologies, conclusions and recommendations can be extended to other populations*”, V. CHARISI, S. CHAUDRON, R. DI GIOIA, R. VUORIKARI, M. ESCOBAR-PLANAS, I. SANCHEZ, E. GOMEZ, *Artificial Intelligence and the Rights of the Child Towards an Integrated Agenda for Research and Policy*, JRC Report, Brussels, 2022, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC127564/JRC127564_01.pdf.

Al fine di costruire un'architettura robusta che protegga la disponibilità, integrità e confidenzialità dei flussi, nulla cambia quando ad essere trattati sono dati, tutti appartenenti a particolari categorie ai sensi dell'art. 9 GDPR. Non è un caso che alcune iniziative legislative extra EU, successive al GDPR, come abbiamo visto, associno addirittura le informazioni personali del minore allo statuto giuridico relativo al trattamento di dati sensibili ⁽⁹⁾.

Per la protezione dei flussi, dunque, l'atteggiamento del sistemista ben potrebbe essere neutrale rispetto alle misure di sicurezza necessarie per tutelare gli accessi, usi e riusi delle informazioni concernenti minori di età, che siano portatori altresì di ulteriori vulnerabilità. A monte, vi sarà una architettura di *governance* differenziata che permetterà o meno l'accesso a/uso e riuso di determinate informazioni piuttosto che di altre, attraverso un approccio progressivamente più granulare rispetto all'informazione specifica che viene processata.

Per la protezione degli altri diritti fondamentali del minore, invero, il sistema di tutele — come abbiamo illustrato nei capitoli precedenti — è multilivello composto sia da illeciti penali, che civili e amministrativi, in cui operatori economici, istituzioni e adulti sono chiamati ad alimentare prioritizzando la funzione preventiva, senza — tuttavia — escludere quella punitiva e compensatoria ⁽¹⁰⁾.

La promozione dei diritti del fanciullo, invece, richiede un altro approccio metodologico: da un lato, possibili azioni positive potrebbero rendersi necessarie per consentire l'accesso alle opportunità della società dell'informazione e delle nuove tecnologie per soggetti minori di età e portatori di ulteriori vulnerabilità, in quanto i bisogni rappresentati richiedono strumenti specifici per fruire di servizi e prodotti digitali; dall'altro lato, invece, la tecnologia può costituire un facilitatore rispetto ai mezzi analogici e alle metodologie intese come tradi-

⁽⁹⁾ L. JASMONTAITE - P. DE HERT, *The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet* (2014) 5 International Data Privacy Law 20 ss.; E. LIEVENS-V. VERDOODT, *Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation* (2018) 34(2) Computer Law & Security Review 269.

⁽¹⁰⁾ Sulle funzioni della responsabilità nel diritto dei consumatori, P. CARTWRIGHT, *Crime, punishment, and consumer protection*, J. Consum Policy, 30, 1-20 (2007). <https://doi.org/10.1007/s10603-006-9026-x>, T. J. HOLT ET AL., *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 1st ed. Cham: Springer International Publishing AG, 2020.

zionali per garantire l'accesso a servizi e prodotti, che altrimenti non potrebbero essere fruiti dal bambino in ragione della propria condizione.

Approfondiremo il tema in tre settori: quello educativo, quello sanitario e nelle attività ludico-ricreative, in modo da provare a fornire degli scenari quanto più vicini alle attività quotidianamente che coinvolgono i bambini.

1.1.1. (Segue). ...e il settore educativo.

Come accennato, la riflessione in ordine al perseguimento dell'interesse superiore del fanciullo portatore di vulnerabilità multiple ben si presta ad essere calata nel settore educativo, che ha la missione di conferire al bambino (*rectius* a tutti i bambini) quelle conoscenze e abilità necessarie per affrontare il futuro.

La fase dell'istruzione obbligatoria e superiore, per esempio, costituisce il momento nella vita della persona umana per acquisire conoscenze e abilità necessarie a consentire di prendere parte attivamente allo sviluppo società, all'economia, e ai processi democratici.

Sul piano della promozione dell'educazione e dell'istruzione del singolo, spetta ai legali rappresentanti, in ragione dell'esercizio delle responsabilità genitoriali ⁽¹¹⁾, perseguire — tenuto conto delle attitudini ed interessi di ciascun bambino — le migliori opportunità di arricchimento culturale dei figli. Spetta, invero, alle istituzioni fornire programmi e occasioni di approfondimento che sviluppino conoscenze e competenze trasversali e arricchiscano il percorso di crescita individuale e della comunità di riferimento. L'organizzazione dell'offerta dei diversi servizi d'istruzione da parte delle istituzioni scolastiche è uno strumento alla portata di tutti per far conoscere le potenzialità tecnologiche esistenti anche alle famiglie e cooperare per la miglior offerta educativa possibile per il singolo bambino. La rapida evoluzione dei sistemi informativi e delle nuove tecnologie spesso, infatti, non è sufficientemente nota al genitore per compiere scelte effettivamente consapevoli, rispetto alle potenzialità che servizi e prodotti potrebbero offrire in termini di recupero, consolidamento o potenziamento delle conoscenze e abilità acquisite o acquisibili ⁽¹²⁾. Per questa ragione,

⁽¹¹⁾ Art. 30 Cost.

⁽¹²⁾ H. HOLMARSDOTTIR, *The Digital Divide: Understanding Vulnerability and Risk in Children and Young People's Everyday Digital Lives*, in H. HOLMARSDOTTIR, I.

soprattutto in questa fase di transizione digitale, importanti investimenti devono essere rivolti all'aggiornamento delle infrastrutture istituzionali e degli educatori al fine di veicolare le risultanze dell'evoluzione in corso, onde evitare che nell'educare e istruire i figli si prendano in considerazione anche mezzi e metodologie offerti dalla società dell'informazione.

Inoltre, la digitalizzazione e l'innovazione tecnologica stanno attuando una vera e propria rivoluzione dei processi organizzativi, amministrativi, e didattici ad ogni livello. L'automazione attraverso sistemi di IA di alcuni passaggi e la spinta verso la dematerializzazione e digitalizzazione consentono, da un lato, di raggiungere un maggior grado di standardizzazione rispetto alla definizione e acquisizione di competenze di base — contribuendo così a incrementare la parità di accesso e trattamento — e, dall'altro lato, di incidere in maniera accurata all'adeguamento delle modalità, tempi, contenuti di erogazione del servizio educativo rispetto ai cc.dd. bisogni speciali, attraverso interventi mirati di personalizzazione ⁽¹³⁾. È proprio in questo processo di personalizzazione che emerge quel valore aggiunto capace

SELAND, C. HYGGEN, M. ROTH (eds) *Understanding The Everyday Digital Lives of Children and Young People*, 2024, Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-46929-9_3; F. DEL BONIFRO, M. GABBRIELLI, G. LISANTI, S.P. ZINGARO (2020). *Student dropout prediction*, in I. I. BITTENCOURT, M. CUKUROVA, K. MULDER, R. LUCKIN, & E. MILLÁN (eds), *Artificial intelligence in education*. Springer International Publishing. https://doi.org/10.1007/978-3-030-52237-7_11, p. 129 ss.

⁽¹³⁾ Come osservato, la questione della costruzione e del rafforzamento di capacità è una sfida che riguarda l'intera società: la tecnologia evolve continuamente e i sistemi educativi non sono attualmente capaci di recepire i bisogni formativi con la stessa rapidità. Ministero della Cultura, *Piano delle attività formative, di ricerca e autovalutazione degli uffici centrali e periferici del Ministero della Cultura 2021-2023*, in <https://dgeric.cultura.gov.it/wp-content/uploads/2021/12/Piano-triennale-delle-attivit -formative-di-ricerca-e-autovalutazione-MiC-2021-2023.pdf>. In letteratura: BENFATTO, M. N., SEIMYR, G.  ., YGGE, J., PANSELL, T., RYDBERG, A., & JACOBSON, C. (2016), *Screening for dyslexia using eyetracking during Reading*, PLoS One, 11(12), e0165508. <https://doi.org/10.1371/journal.pone.0165508>, ASSELBORN, T., CHAPATTE, M., & DILLENBOURG, P. (2020), *Extending the spectrum of dysgraphia: A data driven strategy to estimate handwriting quality*, Scientific Reports, 10(1), 3140. <https://doi.org/10.1038/s41598-020-60011-8>, ALABDULKAREEM, A., ALHAKBANI, N., & AL-NAFJAN, A. (2022), *A systematic review of research on robot-assisted therapy for children with autism*, Sensors, 22(3), 944. <https://doi.org/10.3390/s22030944> Anuradha, J., DHIMAN, T., RAMACHANDRAN, V., ARULALAN, K. V., & TRIPATHY, B. K. (2010), *Diagnosis of ADHD using SVM algorithm*, in Proceedings of the Third Annual ACM Bangalore Conference (pp. 1-4). Association for Computing Machinery. <https://doi.org/10.1145/1754288.1754317>.

di impattare positivamente sulle condizioni di vulnerabilità multipla e di valorizzare gli elementi di diversità che possono emergere al livello individuale (o anche aggregato) in sede di valutazione e monitoraggio dei flussi informativi generati per l'accesso alle risorse educative e la relativa erogazione, nonché per la valutazione dell'apprendimento ⁽¹⁴⁾.

Occorre, tuttavia, riflettere sul possibile carattere invasivo di sistemi basati sull'IA, ad esempio, nelle fasi di selezione degli studenti, nelle loro valutazioni, nonché nella gestione della didattica: dalla selezione dei programmi, al monitoraggio dei comportamenti durante le fasi di valutazione, etc. Per tale ragione il Regolamento europeo sull'IA considera tali sistemi ad alto rischio e richiede la previa analisi dell'impatto sui diritti fondamentali del singolo e dei gruppi ⁽¹⁵⁾. Potendo, infatti, orientare il percorso educativo e professionale della vita di una persona, la decisione automatizzata espone il singolo a implicazioni particolarmente impattanti sulla propria dignità, potendo altresì determinare la possibilità di garantirsi o meno sostentamento. Se i sistemi di IA fossero portatori di *bias* non noti o se fossero utilizzati in maniera impropria, gli stessi potrebbero, ad esempio, riprodurre discriminazioni o crearne di nuove ⁽¹⁶⁾.

Da questo punto di vista, dunque, assume particolare rilievo non tanto il fatto che i servizi educativi siano per lo più erogati a minori di età, quanto piuttosto le possibili vulnerabilità di cui gli studenti sono portatori. In tale contesto, oltre all'appartenenza a minoranze (linguistiche, etniche, religiose, etc.) o a condizioni di disabilità o di barriere

⁽¹⁴⁾ W. HOLMES, I. TUOMI (2022). *State of the art and practice in AI in education*. *European Journal of Education*, 57, 542-570. <https://doi.org/10.1111/ejed.12533>.

⁽¹⁵⁾ §3, Allegato III al Regolamento UE n. 2024/1689, *cit*.

⁽¹⁶⁾ I sistemi di intelligenza artificiale possono, infatti, amplificare o replicare errori o limiti derivanti dai *dataset* con cui vengono addestrati gli algoritmi, soprattutto nelle fasi di valutazione rispetto a forme di scrittura o *background* culturale. Inoltre, laddove gli algoritmi siano costruiti come "scatole nere", diventa difficile ricevere una spiegazione su funzionamento del processo decisionale automatizzato e dunque poterlo comprendere e contestare. Si vedano le osservazioni di V. EUBANKS, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York: St Martin's Press, 2018; F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge: Harvard University Press, 2015, nonché i contributi di ZHANG, J., ZHU, L., ZHU, X., CHENG, Y., ZHU, Y., ZHU, X, *Grading by ai makes me feel fairer? how different evaluators affect college students' perception of fairness*. *Frontiers in Psychology* 15, 1221177 (2024), G. TOLOMEI, F. PINELLI F. SILVESTRI (2022) *Editorial: Human-Interpretable Machine Learning*. *Front. Big Data* 5:956625. doi: 10.3389/fdata.2022.956625.

di tipo culturale, sociale, o economiche, vi potrebbero essere anche vulnerabilità legate a bisogni speciali momentanei, o addirittura legate a caratteristiche di particolari potenziali da non dover assolutamente standardizzare, ma coltivare nella propria individualità.

Le nuove tecnologie svolgono un ruolo prioritario nel supportare la programmazione personalizzata per bisogni educativi speciali legati sia a vulnerabilità note (ad esempio in presenza di una patologia clinica), sia a quelle non necessariamente certificate o certificabili. In particolare, sistemi basati sull'IA ben possono guidare i docenti a disegnare percorsi di insegnamento e di apprendimento a partire dalle diversità rappresentate nel proprio ambiente educativo, non solo macroscopiche — come la presenza di studenti con disturbi cognitivi o appartenenti a minoranze linguistiche — al fine di accogliere, stimolare e sfruttare le differenze nelle attività quotidiane in ottica inclusiva ⁽¹⁷⁾, ⁽¹⁸⁾.

Il potenziale è enorme, tuttavia, occorre distinguere tra le diverse applicazioni. Ad esempio, quelle che possono identificare o inferire emozioni sono considerate ad alto rischio ai sensi del Regolamento sull'IA e, pertanto, soggette a specifici obblighi di trasparenza rispetto all'utente finale: si pensi ad un sistema che possa riconoscere le emozioni dello studente durante lo svolgimento di un compito. L'asimmetria informativa (e di potere) tra studente (soggetto interessato) e la scuola (utilizzatore) esporrebbe, infatti, il primo a rivelare condizioni legate alla propria sfera intima e identitaria, e — dunque — al rischio concreto di usi impropri e arbitrari da parte di utilizzatori con ruoli di valutatori, rendendo il meccanismo controproducente rispetto agli obiettivi educativi e di formazione, oltre che lesivo della dignità e riservatezza della persona ⁽¹⁹⁾.

⁽¹⁷⁾ S. CRAMEROTTI, D. IANES, M. TURRINI, S. LARENTIS, *Un supporto alla programmazione educativo-didattica per gli alunni con BES*, 2015, Trento, Erickson.

⁽¹⁸⁾ Inclusione nel settore educativo significa superare le barriere alla partecipazione all'educazione digitale basata sulle differenze degli studenti e, in particolare, “riconoscer[le], accettar[le] e rispettar[le]”: F. GOTTSCHALK - C. WEISE (2023), *Digital equity and inclusion in education: An overview of practice and policy in OECD countries*, Table 1.1., *OECD Education Working Papers*, No. 299, OECD Publishing, Paris, <https://doi.org/10.1787/7cb15030-en>.

⁽¹⁹⁾ Nel Regno Unito il Dipartimento per l'istruzione ha pubblicato delle raccomandazioni sull'uso dell'intelligenza artificiale generativa nel settore dell'istruzione, facendo riferimento al potenziale degli strumenti di Large Language Models per ridurre il carico di lavoro e migliorare l'insegnamento, ma osservando i limiti rispetto

Alla luce di tali considerazioni etico-giuridiche, lo sviluppo e introduzione di ciascun sistema basato sull'IA nei processi educativi e nel settore istruzione deve essere preceduto da una valutazione di impatto rispetto ai diritti fondamentali della persona e seguire le misure tecnico-organizzative ritenute sufficienti a rendere accettabile l'introduzione di un processo automatizzato nel ciclo di vita educativo. Ciò al fine di promuovere un'istruzione e una formazione digitale di alta qualità e tecnologicamente avanzata, capace di trasmettere abilità e competenze necessarie per affrontare le sfide che la società ci propone oggi e ci proporrà domani nel lavoro, nei servizi, etc ⁽²⁰⁾.

Il settore educativo è, dunque, tra i più sensibili all'evoluzione tecnologica perché capace di intervenire sui processi di alfabetizzazione digitale e sullo sviluppo del pensiero critico degli studenti affinché possano consapevolmente e attivamente prendere parte come cittadini alla vita economica, sociale e democratica. Il bacino d'utenza dei percorsi educativi, peraltro, abbraccia una componente molto vasta di ciascuna comunità di riferimento, includendo, senza distinzioni, bambini nelle fasce di età di istruzione obbligatoria e le proprie famiglie.

Per questo motivo, possono essere disegnate campagne di promozione di sensibilizzazione all'uso responsabile della digitalizzazione e delle tecnologie al di là dei nuovi programmi, non solo per i bambini, ma anche per gli adulti di riferimento (famiglie, educatori, etc.) e di sviluppare risorse specificamente rivolte a gruppi di minori appartenenti anche a determinate fasce di età, che siano portatori di bisogni

all'accuratezza e appropriatezza dei contenuti, richiedendo — pertanto — sempre l'intervento professionale umano per la validazione, nonché le criticità rispetto alla riservatezza e tutela dei dati personali degli utenti e della protezione dei relativi diritti di proprietà intellettuale in caso di contribuzione all'addestramento. Ciò richiama la necessità di sviluppare competenze specifiche e di alfabetizzare prima di introdurre sistemi di IA, The Open Innovation Team and Department for Education, *Generative AI in education Educator and expert views*, 2024, https://assets.publishing.service.gov.uk/media/65b8cd41b5cb6e000d8bb74e/DfE_GenAI_in_education_-_Educator_and_expert_views_report.pdf.

⁽²⁰⁾ A tal proposito, molte organizzazioni internazionali hanno adottato raccomandazioni e linee guida per un uso della tecnologia nel settore educativo, ma l'adeguamento dei programmi presenta *iter* burocraticamente complessi e lunghi per stare al passo con l'evoluzione tecnologica. L'Osservatorio delle *policy* in materia di IA e istruzione dell'OECD raccoglie tutte le *policy* che siano state adottate in materia, classificandole per sistema giuridico, rango, tipologia di investimento e materia, <https://oecd.ai/en/dashboards/policy-areas/PA7>.

speciali — da valorizzare o da supportare — con azioni *ad hoc*, al fine di garantire la parità di trattamento rispetto allo studente medio.

La personalizzazione dell'istruzione attraverso strumenti di IA individua una serie di profili di criticità che devono essere sviscerati per garantire parità di trattamento e inclusività. Da un lato, vi sono le problematiche collegate all'automazione dell'insegnamento, con le implicazioni che possono emergere per il ruolo, la formazione, e il rapporto di lavoro dell'insegnante; poi, vi è la questione collegata alla raccolta, trattamento e monitoraggio dello studente e, in particolare, anche di dati particolarmente sensibili in quanto relativi alla salute, biometrici etc., inoltre l'apprendimento sarebbe valutato come padronanza di un dato argomento rispetto agli *input* forniti alla macchina. Dall'altro lato, assegnare alla macchina compiti di insegnamento, esame e valutazione, tutoraggio per percorsi individualizzati consentirebbe un efficientamento del tempo e delle risorse (umane) dedicate al dato percorso formativo per la comunità ⁽²¹⁾.

In questo contesto, appare ragionevole considerare che l'interesse superiore dei bambini nel settore educativo, al cospetto di possibili vulnerabilità multiple, percorra il duplice binario: quello locale teso a sfruttare le occasioni di crescita nella comunità di riferimento per sviluppare competenze e conoscenze per un uso appropriato ed efficace della tecnologia nella vita quotidiana, e quello istituzionale volto a promuovere la transizione digitale e tecnologica dei servizi educativi di ogni grado di istruzione.

In entrambi i casi, occorre una ferma disponibilità politico-istituzionale ad investire in strumenti e risorse da mettere a disposizione di docenti che possano formarsi in modo da poter trasmettere competenze e conoscenze acquisite e sviluppare nuove metodologie di insegnamento e confronto attraverso l'uso di strumenti messi a disposizione.

1.1.2. (Segue). ...e il settore sanitario.

Un altro settore in cui la minore età del soggetto non costituisce

⁽²¹⁾ W. HOLMES - I. TUOMI (2022), *State of the art and practice in AI*, cit.; B. DU BOULAY (2016), *Artificial intelligence as an effective classroom assistant*, IEEE Intelligent Systems, 31(6), 76-81. <https://doi.org/10.1109/MIS.2016.93>, L. HAKIMI, R. EYNON, & V.A. MURPHY (2021), *The ethics of using digital trace data in education: A thematic review of the research landscape*, in Review of Educational Research, 91(5), 671-717. <https://doi.org/10.3102/00346543211020116>.

l'unica fonte di vulnerabilità è quello sanitario. Due diversi approcci devono essere adottati in ragione del contesto applicativo: infatti, se il bambino ha (anche) una ridotta integrità psicofisica, molte delle riflessioni sulle potenzialità dei servizi e prodotti della società dell'informazione possono costituire strumenti per migliorare la qualità della vita e ridurre le differenze e le discriminazioni. Si pensi — anche alla luce di quanto osservato per il settore educativo — al ruolo degli strumenti di *elearning* o ai programmi di didattica personalizzata a supporto dei bambini con bisogni speciali. In questi scenari, lo strumento tecnologico può costituire un supporto di assistenza, terapeutico o riabilitativo, mentre un determinato servizio digitale può facilitare o stimolare alcune funzioni. In ogni caso, il rapporto tra l'utente bambino e le tecnologie abilitanti viene inquadrato nell'ambito delle misure di sicurezza per l'incolumità fisica e tutela della salute, nonché in relazione ai flussi di dati personali attivati, elaborati ed eventualmente processati dal sistema ⁽²²⁾. Anche in questi casi, più alto è il grado di alfabetizzazione digitale dell'interessato e degli adulti di riferimento, maggiore è la consapevolezza dei possibili usi propri (o meno) che possono essere fatti degli strumenti disponibili.

Quando, invece, si affronta la questione della vulnerabilità multipla dall'altra prospettiva, ovvero quella del paziente che non abbia compiuto la maggiore età, le problematiche si spostano sulle modalità di instaurare e gestire il “*contatto sociale*” nella relazione di cura ⁽²³⁾.

Il fenomeno della datificazione della società nel settore sanitario assume caratteristiche di predittività — ovvero l'avanzamento delle tecnologie consente di elaborare le informazioni del singolo e compararle agli scenari statisticamente più comuni —, migliorando di conseguenza le opportunità di prevenzione, che consentono un sempre più precoce rilevamento di possibili indici di sviluppo di malattie e disturbi. Il che porta a coinvolgere in maniera progressivamente più attiva i pazienti nei processi di diagnosi e cura (c.d. medicina parteci-

(22) S. VISRAM, D. LEYDEN, O. ANNESLEY, ET AL. *Engaging children and young people on the potential role of artificial intelligence in medicine*, in *Pediatr Res* 93, 440-444 (2023). <https://doi.org/10.1038/s41390-022-02053-4>.

(23) F.D. BUSNELLI, *La dimensione della fragilità lungo il percorso della vita umana*, in *Nuovo diritto civile*, 2016; S. CACACE, *Autodeterminazione in salute*, Torino, 2017; V. CALDERAI, *Consenso informato*, in *Enc. dir., Ann.*, Milano, 2015.

pativa) per consentire, altresì, una accurata personalizzazione alle caratteristiche individuali del paziente ⁽²⁴⁾.

In questo quadro, la persona con una ridotta integrità psicofisica (permanente o temporanea) può, grazie alle tecnologie abilitanti, valorizzare la propria dignità attraverso un rinnovato rapporto medico-paziente, che eventualmente può essere mediato dall'interazione con la macchina nelle attività di cura, ma che la rende senz'altro più partecipe. Si pensi alla rilevazione di parametri con strumenti di telemedicina: al paziente non sarà più chiesto di spostarsi in ospedale, ma deve proattivamente contribuire al suo percorso sanitario attraverso lo strumento di rilevazione, assicurandosi che la comunicazione al medico vada a buon fine. Ciò facilita senza dubbio l'attività (eliminando spostamenti, e processi organizzativi collegati, inclusi i costi), ma richiede un certo livello di competenze digitali e attitudine a gestire un ruolo attivo nella relazione di cura a distanza. Inoltre, la tecnologia consente di ridurre direttamente le conseguenze pregiudizievoli di una determinata condizione di salute o disabilità attraverso un miglioramento generale della qualità della vita del paziente ⁽²⁵⁾.

Ciò vale (*rectius* deve valere) anche per il bambino minore di età che abbia una ridotta integrità psicofisica. Lo scenario sanitario diventa un ulteriore esempio di vulnerabilità multipla in cui il supporto digitale e tecnologico si presta a ridurre le barriere determinate dalla specifica fragilità per raggiungere un più alto grado di inclusione sociale ⁽²⁶⁾.

Dal punto di vista tecnico, con riferimento alla gestione delle informazioni nella dimensione digitale, come osservato in premessa, lo statuto giuridico dei dati appartenenti a particolari categorie appare il più adatto a coprire l'esposizione ai rischi derivanti da entrambe le situazioni, senza richiedere ulteriori accorgimenti, essendo già i dati

⁽²⁴⁾ Si parla di *P4 medicine: predictive, preventive, participative, personalised*, cui si aggiunge la quinta caratteristica *psychocognitive*, D. AMRAM, A. CIGNONI, T. BANFI, G. CIUTI, *From P4 medicine to P5 medicine: transitional times for a more human-centric approach to AI-based tools for hospitals of tomorrow*, Open Research Europe, 2022, 2:33, <https://doi.org/10.12688/openreseurope.14524.1>.

⁽²⁵⁾ P.M. ABADIR, R. CHELLAPPA, N. CHOUDHRY, ET AL. *The promise of AI and technology to improve quality of life and care for older adults*. *Nat Aging* 3, 629-631 (2023). <https://doi.org/10.1038/s43587-023-00430-0>.

⁽²⁶⁾ UNICEF Innovation, *Precision health: emerging innovations for children and adolescents*, 2024, <https://www.unicef.org/innovation/media/19681/file/Insights%20Report:%20Precision%20Health%20.pdf>.

sanitari, almeno nell'UE (e anche il dato generico relativo al bambino in alcune esperienze extraeuropee), considerati *per se* sensibili.

È nell'esprimere in concreto un bilanciamento in favore o meno di una determinata tecnologia a supporto della diagnosi, trattamento o riabilitazione che possono emergere ulteriori profili di criticità relativi alla minore età del paziente. Si pensi alle problematiche legate alla gestione del consenso informato, se — quando riferito alla base giuridica del trattamento dei dati personali per un servizio dedicato della società dell'informazione — possa essere espresso direttamente dall'adolescente, senza che ci sia una corrispondente autonomia nel processo decisionale principale, relativo alla prestazione. In questi contesti, da un lato, operano le cc.dd. scelte tragiche⁽²⁷⁾, per cui si demanda a un terzo la risoluzione del conflitto rispetto a possibili opinioni divergenti. Circa il perseguimento dell'interesse superiore del fanciullo, istanza di cui possono farsi portatori i sanitari stessi, interverrà il giudice tutelare a dirimere eventuali controversie⁽²⁸⁾. Dall'altro lato, occorre riflettere anche rispetto al possibile scenario di interazione uomo-macchina, che potrebbe determinare un atteggiamento di eccessiva (o, viceversa, di scarsa) fiducia nella tecnologia, dettato da fattori del tutto estranei alle effettive prestazioni del sistema⁽²⁹⁾.

Laddove, dunque, le tecnologie per la salute e cura della persona siano rivolte al minore di età, al pari degli adattamenti dei requisiti tecnici, legati ai profili fisiologici, sarà necessario introdurre anche elementi organizzativi adattati all'utenza che possano coniugare i bisogni effettivi del paziente con la necessità di proteggerlo da pericoli specifici per il minore di età. Ad esempio, nel caso di limitata locomo-

(27) v. G. CALABRESI - P. BOBBIT, *Le scelte tragiche*, Giuffrè, 2006.

(28) Art. 3, comma 5, legge 2017, n. 219, si riferisce più propriamente al conflitto tra legali rappresentanti del paziente incapace e personale medico sanitario, sebbene al primo comma della medesima disposizione sia espressamente valorizzata la “*capacità di comprensione e di decisione*” del minore di età. Per una lettura in combinato disposto fra i due commi, si veda Tribunale di Modena, decr. 8 febbraio 2022, in *Osservatorio nazionale sul diritto di famiglia*, che ha nominato un curatore speciale per esprimere il consenso ad una emotrasfusione ad un bambino rifiutata dai genitori per motivi religiosi.

(29) JC BJERRING-J. BUSCH, *Artificial intelligence and patient-centered decision-making*, *Philosophy & Technology* 34, 349-371 (2021); BUÇINCA, Z., MALAYA, M. B. & GAJOS, K. Z., *To trust or to think: cognitive forcing functions can reduce overreliance on ai in ai-assisted decision-making*, in *Proceedings of the ACM on Human-Computer Interaction* 5, 1-21 (2021).

zione, appare evidente che l'uso di strumenti digitali consenta al minore di età di compiere una serie di attività educative, ludiche e sociali “da remoto”, occorre tuttavia temperare questa tipologia di opportunità eventualmente facilmente accessibile, con possibili esposizioni a forme di dipendenza, ovvero evitare che l'inclusività digitale non si rifletta in una emarginazione nelle relazioni fisiche o nello sviluppo di dipendenze ⁽³⁰⁾. Questo tipo di temperamento deve poter essere apprezzabile sia dal personale sanitario, che socio-assistenziale, oltre che dai genitori ed adulti di riferimento. In altri termini, l'interesse ad abbattere le barriere — nell'esempio — fisiche, non deve tradursi necessariamente in uno stile di vita inattivo rispetto al mondo fisico e il confine fra uso e uso improprio deve poter essere tracciato caso per caso.

Da questo punto di vista, occorre declinare l'interesse superiore del bambino prendendo in considerazione la situazione nel suo insieme, andando anche ad intervenire in ottica correttiva — o ancor meglio di prevenzione — nel caso concreto, affinché il bilanciamento fra rischi e opportunità sia moderato da chi esercita le responsabilità familiari e dai professionisti che seguono il bambino (vuoi come educatori, vuoi come personale sanitario, etc.). Le ricadute attuative in un sistema di responsabilità multilivello, come quello che abbiamo descritto, sono molteplici: il servizio digitale può fornire dati in ordine alla permanenza della navigazione, laddove gli adulti di riferimento dovranno osservare le effettive conseguenze sulle relazioni quotidiane, il personale sanitario sul benessere psico-fisico, l'educatore sull'apprendimento e sulla base della combinazione delle informazioni occorrerà disegnare una strategia che porti *in primis* a non nuocere, ovvero a limitare il danno ⁽³¹⁾.

⁽³⁰⁾ G. QUAGLIO, S. MILLAR, *Potentially negative effects of Internet Use*, European Parliament Research Service, 2022. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641540/EPRS_IDA\(2020\)641540_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/641540/EPRS_IDA(2020)641540_EN.pdf), più di recente A. RIMMERMAN, 'Social Inclusion of People with Disabilities: Current Approaches and Perspectives', *Social Inclusion of People with Disabilities Revisited: Perspectives Reflected by the COVID-19 Pandemic* (New York, NY, 2024; online edn, Oxford Academic, 19 Sept. 2024), <https://doi.org/10.1093/9780197758939.003.0002>.

⁽³¹⁾ I. MARINO, G. DI NAPOLI, A. GENTILE, C. NOVARA (2024). *Adolescents as the Vulnerable Users of Digital Technologies - Relationship Between Vulnerable Narcissism and Community Sense*. In Book of Abstract. Psychology and Behavioral Science, 1-10.

2. Muoversi attorno al piano dell'autonomia e della consapevolezza del singolo: il ruolo della trasparenza.

Nei capitoli precedenti abbiamo analizzato come l'offerta di servizi e prodotti digitali sia accessibile e fruibile a minori di età che appartengono a fasce di età diverse, con conseguenti implicazioni sia sulla capacità di determinare il proprio comportamento *online*, sia rispetto ai rischi di esposizione a pericoli per l'incolumità, la salute e la sicurezza.

Il profilo reciproco (e complementare rispetto a quello analizzato) riguarda l'impatto della dimensione digitale sui processi di apprendimento, sullo sviluppo dell'autonomia di pensiero e sulla capacità decisionale dei minori di età, in ottica costruttiva rispetto alla maturità psico-fisica della futura persona adulta del domani. Il riconoscimento di forme anticipate di autonomia decisionale per i servizi della società dell'informazione, seppur limitata agli adolescenti, deve essere accompagnato da un adattamento degli strumenti informativi previsti per gli adulti, non solo per far adempiere responsabilmente il titolare del trattamento agli obblighi di trasparenza in ordine alle attività di processamento delle informazioni personali, rendendo comprensibile e alla portata del giovane utente i dettagli relativi alla natura, mezzi, finalità, durata etc. dei trattamenti, ma anche per responsabilizzare l'utente minorenne stesso a prendere decisioni consapevoli in contesti che siano — in ragione delle misure tecnico-organizzative — sicuri *by design* e *by default* ⁽³²⁾.

In altri termini, la maggiore indipendenza e autonomia che gli adolescenti assumono nella dimensione digitale costituisce un innovativo banco di prova per sviluppare la propria personalità attraverso l'assunzione di ruoli e responsabilità verso se stessi e verso gli altri. Torna il paragone con la circolazione stradale: finché il bambino è accompagnato per mano dagli adulti si lascia guidare. Comincia ad orientarsi al momento in cui si trova a dover raggiungere obiettivi ogni volta più distanti e comincia a sviluppare indipendenza e conseguente capacità di prevenire i pericoli, soprattutto nel momento in cui utilizza un mezzo proprio (dal triciclo, alla bicicletta, sino al ciclomotore), in quanto comprende di dover preservare non solo se stesso, ma anche gli

⁽³²⁾ M.E. KAMINSKI, *Understanding Transparency in Algorithmic Accountability*, in Barfield W, ed. *The Cambridge Handbook of the Law of Algorithms*. Cambridge Law Handbooks. Cambridge University Press; 2020:121-138.

altri ⁽³³⁾. Per colmare il divario esperienziale tra un adulto e un minore rispetto alla prevedibilità delle conseguenze di una determinata azione occorre educare e formare alle regole della strada e della convivenza civile e informare con la segnaletica appropriata (e universale) per consentire di intraprendere la scelta corretta nello scenario specifico.

Orbene, nella dimensione digitale, è la trasparenza nelle sue declinazioni di misura tecnica e misura organizzativa a giocare il ruolo prioritario di bussola orientativa per colmare l'asimmetria informativa tra operatori economici (e non solo: si pensi al personale sanitario) e l'utente. Gli adattamenti per consentire al minore di età di essere reso edotto e comprendere il funzionamento della applicazione e il relativo trattamento dei dati impongono di utilizzare un linguaggio semplice e comprensibile ⁽³⁴⁾: il che significa fornire testi più brevi e con icone o immagini di accompagnamento alla lettura che veicolino il messaggio in maniera inequivocabile per (tutti) i bambini, al pari della segnaletica stradale. A tal fine, tecniche di *legal design* possono creare i contenuti più facilmente accessibili e inclusivi ⁽³⁵⁾.

Diversamente, la trasparenza intesa come principio tecnico riguarda i processi di verifica delle decisioni automatizzate al fine di poterne correggere gli effetti, laddove siano distorsivi rispetto ai principi di inclusività e non-discriminazione, oppure siano lesivi di diritti

⁽³³⁾ H. WEIR, *Children's autonomous mobility and their well-being*, Wellbeing, Space and Society, Volume 4, 2023, 100134, ISSN 2666-5581, <https://doi.org/10.1016/j.wss.2023.100134>, che richiama gli studi sulle implicazioni della *Self Determination theory*: R. M. RYAN, E. L. DECI, *Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions*, Contemporary Educational Psychology, Volume 61, 2020, 101860, ISSN 0361-476X, <https://doi.org/10.1016/j.cedpsych.2020.101860>.

⁽³⁴⁾ EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 maggio 2020.

⁽³⁵⁾ Sulle frontiere del *legal design*, si vedano i contributi in R. DUCATO-A. STROWEL (a cura di), *Legal Design Perspectives: Theoretical and Practical Insights from the Field*, Ledizioni, 2021, disponibile in open access, a questo link: https://aura.abdn.ac.uk/bitstream/handle/2164/18146/Ducato_Strowel_Legal_Design_Perspective_Book_VOR.pdf;jsessionid=C45F814E8122094B98E1FF5B70046AFC?sequence=1, per un approfondimento tecnico, S. HUMAN, H. J. PANDIT, V. P. MOREL, C. SANTOS, M. DEGELING, A. ROSSI, W. BOTES, V. JESUS, I. KAMARA, *Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenge*, 2021 2022, 7th IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2022): Proceedings. Genoa, Italy: IEEE, p. 231-239. Si veda infine il Manifesto R. DUCATO, H. HAPIO, M. HAGAN, M. PALMIRANI, S. PASSERA, A. ROSSI, *The Legal Design Manifesto v.1*, 2018, <https://www.legaldesignalliance.org>.

fondamentali della persona (come singolo, o come appartenente a un gruppo), oppure non corrispondano agli esiti previsti o non siano sufficientemente accurati ⁽³⁶⁾. Protagonisti di questo processo non sono solo gli sviluppatori, in quanto debbono essere coinvolti i portatori di interessi nelle fase di allenamento, test e validazione, che — pertanto — devono essere messi nelle condizioni di partecipare attivamente e con consapevolezza anche alle vicissitudini tecniche del trattamento dei dati e delle informazioni che li riguardano. Da questa prospettiva il principio di trasparenza si collega alle esigenze di spiegabilità dei processi automatizzati ⁽³⁷⁾.

Costruire una cittadinanza digitale ⁽³⁸⁾ significa, tuttavia, non solo formare all'uso delle tecnologie, attraverso conoscenze specifiche in ambito di protezione dei flussi di dati, cybersicurezza e programmazione, ma altresì sviluppare competenze trasversali per consentire ai cittadini tutti — minori di età inclusi — di comprendere i meccanismi adottati dai processi automatizzati, mediante l'esercizio di un consapevole diritto alla spiegabilità ⁽³⁹⁾ per finalità non solo di validazione, ma anche — laddove necessario — per responsabilmente contestarne la metodologia o gli esiti ⁽⁴⁰⁾.

L'interesse superiore del bambino rispetto al diritto all'informazione quale espressione della trasparenza al fine di sviluppare contezza e consapevolezza rispetto ad attività digitali si raggiunge attraverso la conformità agli obblighi di trasparenza da parte degli operatori e la

⁽³⁶⁾ E. YADOLLAHI, M. LIGTHART, K. SHARMA, E. RUBEGNI, *Explainable and Transparent Child-Technology Interaction*, 2024, ACM, NY, 1016 ss., doi: 10.1145/3628516.3661151.

⁽³⁷⁾ K. WEITZ, D. SCHILLER, R. SCHLAGOWSKI, ET AL. "Let me explain!": exploring the potential of virtual agents in explainable AI interaction design. *J Multimodal User Interfaces* 15, 87-98 (2021). <https://doi.org/10.1007/s12193-020-00332>, A. SIMONCINI, *L'algoritmo incostituzionale, intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 2019, p. 63 s.

⁽³⁸⁾ L'iniziativa è del Consiglio d'Europa per promuovere una educazione volta a costruire una cittadinanza digitale: 2025 European Year of Digital Citizenship Education (DCEY2025), <https://rm.coe.int/dcey2025/1680aca832>.

⁽³⁹⁾ F. GIANNOTTI, F. NARETTO, F. BODRIA, *Explainable for trustworthy AI*, in *Human-Centered Artificial Intelligence: Advanced Lectures*, in M. CHETOUANI V. DIGNUM, P. LUKOWICZ, C. SIERRA (eds) Springer, 2023, 175 ss.

⁽⁴⁰⁾ JOBIN, A., IENCA, M. & VAYENA, E. *The global landscape of AI ethics guidelines*. *Nat Mach Intell* 1, 389-399 (2019). <https://doi.org/10.1038/s42256-019-0088-2>, ALFRINK, K., KELLER, I., KORTUEM, G. ET AL. *Contestable AI by Design: Towards a Framework*, *Minds & Machines* 33, 613-639 (2023).

comunicazione degli esiti attraverso un linguaggio alla portata di bambino, preferibilmente adattato alla fascia di età dei soggetti interessati e del grado di autonomia. Gli operatori economici sono dunque chiamati a utilizzare strumenti e metodologie di comunicazione e informazione adatte all'età e alla capacità di discernimento dell'utente, prevedendo meccanismi di verifica della comprensione — specialmente dei rischi — rispetto all'uso (più o meno prolungato) di una determinata soluzione, laddove — ad esempio — il minore non sia supportato da un educatore o da un adulto nella fruizione del servizio o del prodotto.

A questo proposito, tuttavia, occorre prestare attenzione alle criticità sollevate in materia di sovraccarico informativo che, se dal lato del contraente forte assicura l'adempimento a obblighi di trasparenza, a ciò non corrisponde sempre una effettiva comprensione dei contenuti oggetto della comunicazione. Non sempre, inoltre, è sufficiente che il contraente debole sia solo messo nelle condizioni di conoscere le caratteristiche del servizio e dei trattamenti dei dati ad esso connesso, potrebbe rivelarsi, invero, necessario intervenire durante l'utilizzo per evitare l'esposizione a pericoli o le relative conseguenze pregiudizievoli ⁽⁴¹⁾.

Un alleggerimento, a fini di *accountability*, dell'onere di provare di aver fornito informative alla portata degli utenti minorenni potrebbe essere previsto in caso di evidente (e certificata) conoscenza specifica dei servizi della società dell'informazione e delle nuove tecnologie. Ad esempio, nel caso di adozione e utilizzo del proposto patentino digitale, informative *standard* potrebbero essere sufficienti a garantire la comprensibilità da parte dell'utente minorenne che abbia acquisito competenze e conoscenze specifiche in materia. D'altro canto, tuttavia, una progressiva maggiore autonomia nella dimensione digitale richiede non solo una alfabetizzazione generalizzata, ma soprattutto una avanzata e continua educazione (al) digitale.

(41) Fornire informazioni superflue e non utili per il consumatore è considerata una sorta di manipolazione, fallendo nell'obiettivo di proteggere: O. BAR-GILL - O. BEN-SHAHAR, *Misprioritized Information: A Theory of Manipulation*, J. Leg. Studies, 52, 2 e ancor prima, O. BEN-SHAHAR & C. E. SCHNEIDER, *The Failure of Mandated Disclosure* (2017) 2017 Actual Probs Econ & L 146, O. BEN-SHAHAR, *The Myth of the 'Opportunity to Read' in Contract Law* (2009) 5(1) European Review of Contract Law 1.

3. L'educazione digitale: rafforzare conoscenze e competenze tecnologiche.

Nei paragrafi precedenti abbiamo analizzato l'impatto delle vulnerabilità multiple nel settore educativo e accennato al ruolo della c.d. *digital literacy*, come pilastro per una responsabilizzazione dei cittadini all'utilizzo responsabile di sistemi basati sull'IA ⁽⁴²⁾.

L'educazione digitale e al digitale, infatti, permette di completare il quadro di misure di protezione e promozione dei valori dell'UE e dei diritti fondamentali della persona rispetto alle criticità lanciate dalla digitalizzazione e dall'innovazione tecnologica. A questo proposito, la Commissione Europea ha lanciato il Digital Education Plan (2021-2027) come insieme di iniziative che convergono sulla possibilità di creare un percorso di rafforzamento e riconoscimento di specifiche competenze e abilità digitali che possa costituire uno *standard* applicabile in tutti gli Stati Membri attraverso il rilascio di una certificazione che attesti il livello conseguito dal singolo cittadino ⁽⁴³⁾.

Alla luce delle considerazioni svolte nei precedenti paragrafi, questo piano di educazione digitale ben si presterebbe a incorporare la proposta di sviluppare uno schema di certificazione alla portata dei bambini e degli adolescenti per poter supportare le famiglie e le scuole nei compiti di cura e istruzione nella dimensione digitale, attraverso corsi tenuti da personale a sua volta certificato nell'ambito dello schema, garantendo la possibilità di far sostenere esami di valutazione al completamento dei singoli moduli, sino ad ottenere il proposto "patentino digitale".

Al fine di utilizzare questo meccanismo nella popolazione minorile appare utile implementare due azioni: in primo luogo, verificare l'adequatezza dei programmi ai bisogni educativi degli utenti minorili a seconda della fascia di età e, in secondo luogo, coinvolgere le scuole affinché possano erogare — attraverso personale accreditato

⁽⁴²⁾ La definizione di alfabetizzazione digitale secondo l'approccio olistico dell'UNICEF si riferisce "*alle conoscenze, alle competenze e agli atteggiamenti che consentono ai bambini di prosperare e irrobustirsi in un mondo digitale sempre più globale, essendo sia sicuri che autonomi, in modi appropriati alla loro età e alle culture e ai contesti locali*", UNICEF, *Digital literacy for children: exploring definitions and frameworks*, 2020, <https://www.unicef.org/globalinsight/media/1271/file/%20UNICEF-Global-Insight-digital-literacy-scoping-paper-2020.pdf>.

⁽⁴³⁾ European Digital Skills Certificate, <https://education.ec.europa.eu/focus-topics/digital-education/action-plan/action-9>.

secondo lo schema di certificazione — corsi (possibilmente gratuiti col supporto delle istituzioni) — collegati al piano formativo adottato dalla Commissione Europea. Cinque sono le aree di competenza individuate nel Digital Education Plan, ciascuna articolata su quattro livelli di specializzazione (base, intermedio, avanzato e altamente specializzato): *i*) informazione e alfabetizzazione in materia di dati, *ii*) comunicazione e collaborazione *iii*) costruzione di contenuti digitali, *iv*) sicurezza, *v*) risoluzione di problemi ⁽⁴⁴⁾.

La sfida per una dimensione digitale a portata di fanciullo dovrebbe consistere nell'articolare programmi e materiali per consentire di acquisire competenze e conoscenze sulle medesime aree anche ai bambini e agli adolescenti, valorizzando gli elementi di diversità che possono caratterizzare le comunità di riferimento in quel particolare momento storico. Ciò per promuovere l'accesso alle risorse della società dell'informazione, consentire di utilizzare i servizi e le tecnologie, stimolando progressivamente sensibilità e responsabilizzazione attraverso la formazione di capacità critica rispetto al riconoscimento di rischi e pericoli da prevenire e le opportunità da cogliere.

Volendo mantenere la metafora della graduale acquisizione di autonomia e indipendenza su strada, potremmo considerare l'evoluzione del bambino che passa dall'essere trasportato in un seggiolino sulla bicicletta del genitore, al poter pedalare su quattro ruote, fino ad imparare ad andare in bicicletta autonomamente. In ciascuna fase, ci sono obiettivi minimi da raggiungere con regole da seguire differenziate sulla base del livello di responsabilità e affidabilità riconosciuti al minore stesso nel muoversi nell'ambiente circostante. Dapprima il bambino potrà usare la bicicletta solo per passeggiate con adulti, acquisendo poi autonomia per tragitti brevi e/o su strade poco trafficate, fino a potersi muovere ovunque, anche senza supervisione diretta dell'adulto.

La metodologia di apprendimento e di acquisizione di autonomia appare essere la medesima: occorre cambiare gli strumenti adattandoli alla transizione digitale della realtà circostante e alle esigenze di apprendimento dei bambini.

(44) R. VUORIKARI, S. KLUZER, Y. PUNIE, *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48883-5, doi:10.2760/490274, JRC128415.

In quest'ottica, l'alfabetizzazione digitale e in materia di intelligenza artificiale si iscrive nei processi educativi come misura organizzativa volta a proteggere e promuovere gli interessi superiori degli utenti minorenni e a fornire loro quelle competenze che consentono di rendersi progressivamente più consapevoli rispetto ad un uso responsabile delle tecnologie e della dimensione digitale come occasioni di realizzazione della propria persona.

4. Nuove tecnologie, gioco e creatività.

Un profilo di notevole importanza nel trattare l'interesse superiore del bambino è quello relativo al diritto al gioco nella dimensione digitale, che deve lasciare spazio alla sperimentazione individuale per consentire un continuo stimolo della fantasia e dei meccanismi di risoluzione di problemi ⁽⁴⁵⁾.

La transizione digitale delle attività ludiche e ricreative richiede ancor più che in altri settori che l'ambiente dedicato sia sicuro e inclusivo. In particolare, i giochi debbono evitare di indurre l'utente a comportamenti discriminatori, violenti verso altri coetanei. Misure di salvaguardia devono contestualmente preservare gli utenti dallo sviluppare disturbi, come forme di dipendenza e verificare che i contenuti proposti siano allineati rispetto alla fascia di età rappresentata dagli utenti e alle aspettative di sviluppo psicofisico degli stessi, incoraggiando l'uso di creatività e immaginazione. Studi recenti, infatti, sottolineano come sia indispensabile coinvolgere il minore di età in attività di sperimentazione che lo stimolino a prendere il controllo dei possibili percorsi e scenari di gioco e contribuiscano allo sviluppo della capacità di discernimento, includendo quelle strumentali all'acquisizione di abilità di supervisione umana rispetto ai processi decisionali automatizzati della macchina, nonché quelle orientate a sollecitare creatività e fantasia. In altri termini, attraverso il gioco nella dimensione digitale non solo si garantisce l'attuazione dell'art. 31 CRC, ma allo stesso

⁽⁴⁵⁾ S. LIVINGSTONE, E. LIEVENS, J. CARR, *Handbook for policy makers on the rights of the child in the digital environment*, CoE - Strasburgo, 2021, <https://rm.coe.int/handbook-for-policy-makers-on-the-rights-of-the-child-in-the-digital-e/1680a069f8>.

tempo si contribuisce alla missione di acquisizione di consapevolezza e competenze digitali ⁽⁴⁶⁾.

Come limite, vi è la responsabilità condivisa tra adulti di riferimento e prestatori di servizi digitali di evitare condotte abusive da parte del bambino, specialmente della permanenza nella dimensione digitale. Si parla a tal proposito di diritto alla disconnessione ⁽⁴⁷⁾: abbiamo osservato come alcuni stati USA avessero introdotto divieti di utilizzo di piattaforme digitali in certe fasce per consentire il fisiologico riposo notturno del bambino ed evitare l'emergere di forme di dipendenza. Altre misure — meno invasive — orientate a tutelare il diritto alla disconnessione e implementabili nei sistemi messi a disposizione dei bambini attraverso le funzionalità di controllo parentale consistono nel richiedere di trasmettere notifiche con statistiche periodiche relative alla permanenza *online* del dispositivo, oppure al superamento di una certa soglia nell'arco di un certo lasso di tempo, oppure di introdurre dei blocchi che obblighino alla disconnessione dei dati superato un certo limite di utilizzo prestabilito.

Oltre a quelle legate allo sviluppo di dipendenze, un'ulteriore problematica riguarda il dibattito in ordine alle implicazioni relative all'utilizzo di sistemi basati sull'IA sulla creatività. A fronte di efficienza e standardizzazione legate all'automazione di processi, infatti, il rischio di appiattire il guizzo creativo appare particolarmente attuale, specialmente laddove si tratti di sistemi capaci di creare nuovi contenuti, in qualsiasi formato, come nel caso dell'IA generativa ⁽⁴⁸⁾. Recenti studi hanno dimostrato che l'uso di IA di tipo generativo, per esempio, incrementa la creatività individuale, migliorando i tempi per lo sviluppo

(46) Tali principi emergono da uno studio condotto in un totale di 1933 bambini tra 6 e 17 anni sulla comparazione tra la qualità del gioco nella dimensione virtuale e in quella digitale: DIGITAL FUTURE COMMISSION, *Playful by design. Free Play in a Digital World*, 2021, <https://digitalfuturescommission.org.uk/wp-content/uploads/2021/11/DFC-Playful-by-Design-survey-report-and-findings.pdf>.

(47) Tra le prime riflessioni in materia D. POLETTI, *Il c.d. diritto alla disconnessione nel contesto dei "diritti digitali"*, in *Resp. civ. prev.*, 2017, 8 ss. Il concetto è stato poi legato allo stress da lavoro correlato in tempi di gestione della pandemia, M.C. CATAUDELLA, *Tempo di lavoro e tempo di disconnessione*, in *Mass. giur. lav.*, 2021, p. 853 s.

(48) J. RAFNER, R.E. BEATY, J.C. KAUFMAN ET AL., *Creativity in the age of generative AI*, *Nature Hum Behav* 7, 1836-1838 (2023). <https://doi.org/10.1038/s41562-023-01751-1>. Sulle problematiche connesse al diritto d'autore, C. SGANGA, *Is There Still a Policy Agenda for EU Copyright Law?* (2023) *International Review of Intellectual Property and Competition Law*, 54. pp. 1407-1417.

di contenuti, ma diminuisca la diversità e, più in generale, la novità al livello aggregato ⁽⁴⁹⁾. Altri sostengono che debba essere ridisegnato il concetto stesso di creatività, utilizzando gli strumenti di IA per scomporre, gestire e interpretare, ad esempio, la musica, le immagini, i colori, le parole o i materiali affinché gli artisti possano esplorare in modo più efficace come ampliare la loro capacità di espressione personale ⁽⁵⁰⁾.

Calando queste considerazioni nel processo evolutivo dei bambini, la sfida da cogliere è senz'altro quella di creare competenze e capacità per un innalzamento degli *standard* di base che renda gli strumenti più avanzati accessibili a tutti, ma occorre — al contempo — preservare e poter valorizzare il contributo personale e diversificato di ciascuno ⁽⁵¹⁾, enfatizzando il ruolo di supporto e di organizzazione di contenuti, più che di generazione di idee ⁽⁵²⁾.

In quest'ottica, non è un caso che i primi studi volti ad esplorare le potenzialità dell'uso di strumenti di IA per stimolare la creatività e le abilità di formazione di pensiero critico nei bambini siano stati avviati

⁽⁴⁹⁾ Nella specie, l'esperimento riguardava la scrittura di brevi racconti con il supporto di ChatGPT4, cfr. A. R. DOSHI, O.P. HAUSER, *Generative AI enhances individual creativity but reduces the collective diversity of novel content*, Sci. Adv.10, eadn5290 (2024), doi:10.1126/sciadv.adn5290. Un altro studio condotto al MIT, invece, si riferisce alla produttività di coloro che sono impiegati in attività di scrittura: S. NOY, W. ZHANG, *Experimental evidence on the productivity effects of generative artificial intelligence*, Science, 381, p. 187-192 (2023). doi:10.1126/science.adh2586. Si è dimostrato che ChatGPT ha aumentato la qualità dei risultati delle attività di scrittura dei lavoratori laureati con minor capacità, riducendo i tempi di impiego, riducendo — al livello aggregato — le differenze tra i diversi livelli di professionalità.

⁽⁵⁰⁾ Per il settore musicale, C. A. HUANG, H. V. KOOPS, E. NEWTON-REX, M. DINCULESCU, C. CAI, *AI song contest: Human-AI co-creation in songwriting*, in *Proceedings of the 21st International Society for Music Information Retrieval Conference*, p. 708, Montreal, Canada, <https://zenodo.org/badge/DOI/10.5281/zenodo.4245530.svg>; F. VINCHON ET AL. *J. Creat. Behav.* <https://doi.org/10.1002/jocb.597> (2023).

⁽⁵¹⁾ Un primo passo in questa direzione è legato alla sensibilizzazione ai contenuti palesemente falsi generati da sistemi di AI, sul punto si veda S. ALI, D. DI PAOLA, I. LEE, V. SINDATO, G. KIM, R. BLUMOFFE, C. BREAZEAL, *Children as creators, thinkers and citizens in an AI-driven future*, *Computers and Education: Artificial Intelligence*, Volume 2, 2021, 100040, ISSN 2666-920X, <https://doi.org/10.1016/j.caeai.2021.100040>.

⁽⁵²⁾ Sono note le posizioni di Chomsky che definisce AI e Language Models come “*plagiarism software because it doesn't create anything, but copies existing works of existing artists modifying them enough to escape copyright laws*”, così N. CHOMSKY on ChatGPT, Education, Russia and the unvaccinated, 20 gennaio 2023, <https://www.youtube.com/watch?v=IgxzcOugvEI&t=250s>.

nelle scuole e, più in generale, nel settore educativo ⁽⁵³⁾. Le evidenze sono ancora allo stato preliminare, pertanto, in questa fase, occorre che la questione di preservare e promuovere la creatività del singolo a fronte di un supporto della tecnologia ad attivare certi stimoli sia misurato caso per caso nell'ambito delle valutazioni di impatto dei diversi strumenti che possono essere introdotti.

5. Promuovere la sfera relazionale e quella emotiva.

La datificazione della società impatta notevolmente sui meccanismi di comunicazione e, di conseguenza, sulle relazioni personali e familiari ⁽⁵⁴⁾. Occorre comprendere, in ottica necessariamente interdisciplinare rispetto a studi sociologici, psicologici e antropologici, quali azioni dirette a bambini, famiglie ed educatori possano agire in maniera complementare rispetto agli obblighi imposti agli operatori economici di tutela *by design* e *by default* per prevenire ed evitare situazioni patologiche (dal cyberbullismo alla dipendenza) e quali meccanismi si rendano necessari per invece promuovere il perseguimento di opportunità di crescita emotiva e relazionale grazie all'uso delle tecnologie.

Come evidenziato, un uso improprio dei servizi della società dell'informazione può recare pregiudizi alla salute e incolumità dell'utente: ad esempio, può indurre il bambino a sviluppare disturbi comportamentali, patologie, e dipendenze. I meccanismi di controllo parentale possono fornire informazioni circa i tempi e i luoghi della navigazione di uno specifico *account* o l'uso di una applicazione tecnologica e introdurre meccanismi di blocco. Queste misure tecniche, tuttavia, possono essere necessarie e sufficienti per certe problematiche, ma costituire solo una parte della più complessa questione legata alla transizione digitale di relazioni interpersonali e allo spazio virtuale come dimensione ove (poter o dover) gestire o mostrare le emozioni ⁽⁵⁵⁾.

⁽⁵³⁾ L. EUM LEE, *Metaphor analysis on pre-service early childhood teachers' conception of AI (Artificial Intelligence) education for young children*, Thinking Skills and Creativity, 2024, Elsevier, doi: 10.1016/j.tsc.2023.101455, Y. ZIHAN ET AL., *Na-Canva: Exploring and Enabling the Nature-Inspired Creativity for Children*, Proceedings of the ACM on human-computer interaction 7.MHCI (2023): 1-25. Print.

⁽⁵⁴⁾ F. PIRA, *Figli delle App.*, cit.

⁽⁵⁵⁾ *Ibidem*.

Si tratta di comprendere fino a che punto la dimensione digitale possa costituire un mero luogo di scambio di comunicazioni interpersonali e come ciò influisca sullo sviluppo psicofisico del bambino.

Si pensi, a tal proposito, al fenomeno dell'uso dell'ambiente virtuale in cui un *avatar*, prendendo le sembianze di un soggetto reale, può manifestarsi in maniera del tutto conforme o difforme rispetto alla persona fisica che fornisce istruzioni e ne determina azioni e comportamenti, come nel caso del Metaverso ⁽⁵⁶⁾. La problematica abbraccia, da un lato, l'ipotesi di concepire come reale o finzione lo spazio virtuale, con la conseguenza che certe condotte possano o meno produrre effetti giuridici rilevanti ⁽⁵⁷⁾, ⁽⁵⁸⁾. Dall'altro lato, ci si interroga su come coniugare questi profili con lo sviluppo emotivo del bambino.

Altri studi dimostrano che le tecnologie digitali siano utili per

⁽⁵⁶⁾ A. KÜSTERS, *A Tale of Two Metaverses: Assessing the EU's Influence on Standard-Setting in Virtual Worlds* (2024) Proceedings of the International Congress Towards a Responsible Development of the Metaverse, Alicante, 13-14 June, 2024.

⁽⁵⁷⁾ In alcuni casi, nel Metaverso si sono conclusi contratti, ovvero si sono celebrati matrimoni. La sfida è comprendere se tali attività siano giuridicamente rilevanti, se necessitino di una sorta di conversione nello spazio reale, valendo come attività negoziali precontrattuali da eseguirsi — in ogni caso — secondo buona fede, oppure se vi sia la possibilità o necessità di convertire attraverso trascrizioni dello scambio di volontà. In particolare, non essendo il metaverso disciplinato da uno specifico sistema giuridico, le parti ben potrebbero — nell'ambito della relativa autonomia — scegliere la legge applicabile e decidere di contrarre nel Metaverso sulla base di una interpretazione della Convenzione di onvenzione sulla legge applicabile alle obbligazioni contrattuali aperta alla firma a Roma il 19 giugno 1980 (c.d. Convenzione Roma I). Diversamente, per atti pubblici, come potrebbe essere contrarre matrimonio o unione civile, occorre che il sistema lo permetta con una disposizione di rango primario, M. ZANELATO, *Questo matrimonio s'ha da fare (nel Metaverso). Nuovi luoghi, stesse persone*, *Journal of Ethics and Legal Technologies*, 2023, 5(2), 61-80. doi: 10.14658/pupj-JELT-2023-2-4. Per un approfondimento, si veda lo studio del Parlamento Europeo, finanziato dal JURI Committee: M. MACIEJEWSK, *Metaverse*, 2023, [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU\(2023\)75122_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/751222/IPOL_STU(2023)75122_EN.pdf), J. GÓMEZ-QUINTERO, S. D. JOHNSON, H. BORRION, S. LUNDRIGAN, *A scoping study of crime facilitated by the metaverse*, *Futures*, Volume 157, 2024, 103338, <https://doi.org/10.1016/j.futures.2024.103338>.

⁽⁵⁸⁾ Dal punto di vista penale, invece, si parla di trasposizione in ambiente digitale del *locus commissi delicti* e della natura transfrontaliera del reato, cfr. A. CONTINIELLO, *Le nuove frontiere del diritto penale nel Metaverso. Elucubrazioni meta-giuridiche o problematica reale?*, in *Giurisprudenza Penale*, 2022, 5, p. 1 ss.

mantenere le relazioni familiari, in caso di separazione dei nuclei familiari per qualsivoglia motivo ⁽⁵⁹⁾.

L'eventuale profilazione degli utenti sulla base delle emozioni riconosciute e individuate da tecnologie basate sull'IA, infatti, ben possono esporre — più che gli adulti — a pratiche manipolative non solo pregiudizievoli rispetto all'eventuale autonomia contrattuale in ottica consumeristica, ma anche rispetto alle relazioni affettive che potrebbero minare il fisiologico sviluppo della persona.

Studi psicologici dimostrano l'efficace apporto delle nuove tecnologie a fini terapeutici e riabilitativi nella gestione delle emozioni in pazienti con disturbi mentali e neurologici ⁽⁶⁰⁾, ma dimostrano altresì che l'esposizione non controllata possa alimentare attitudini fino a sfociare in disagi nuovi o peggiorare situazioni già esistenti. In particolare, si nota che l'uso passivo di piattaforme digitali e *social network* possano collegarsi ad un aumento dei livelli di depressione, bassa autostima e solitudine, cui si associa una ridotta attività fisica e, più in generale, del benessere ⁽⁶¹⁾.

⁽⁵⁹⁾ Si pensi al programma di elearning lanciato dall'UNICEF per i bambini ucraini, UNICEF, *Back to school for Ukrainian children at Digital Learning Centers*, 2023, <https://www.unicef.org/ukraine/en/stories/back-to-school-for-ua-children-at-digital-learning-centers>.

⁽⁶⁰⁾ B. DEL LUCCHESI, S. PARRAVICINI, S. FILOGNA, G. MANGANI, E. BEANI, MC DI LIETO, A. BARDONI, M. BERTAMINO, M. PAPINI, C. TACCHINO, F. FEDELI, G. CIONI, G. SGANDURRA AND THE ITALIAN NEUROSCIENCE AND NEUROREHABILITATION NETWORK (2024) *The wide world of technological telerehabilitation for pediatric neurologic and neurodevelopmental disorders - a systematic review*, in *Front. Public Health* 12:1295273. doi: 10.3389/fpubh.2024.1295273 e E. BEANI, S. FILOGNA, G. CIONI, G. SGANDURRA (2023) *From the Early Detection to Early Intervention at Home: The Role of Technology in Infancy*, in L. PROVENZI, S. GRUMI, R. BORGATTI (a cura di), *Family-Centered Care in Childhood Disability*. Springer, Cham. https://doi.org/10.1007/978-3-031-34252-3_5.

⁽⁶¹⁾ Tra gli effetti più comuni negli adolescenti si notano: sbalzi d'umore estremi, uso di sostanze nocive, disturbi del sonno, difficoltà di concentrazione, etc., si vedano gli studi condotti da T. CHEN, J. OU, G. LI, H. LUO, *Promoting mental health in children and adolescents through digital technology: a systematic review and meta-analysis*. *Front Psychol.* 2024 Mar 12;15:1356554. doi: 10.3389/fpsyg.2024.1356554. PMID: 38533221; PMCID: PMC10963393 e un meno recente report dell'UNICEF curato da D. KARDEFELT-WINTHER, *How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity?*, 2017, <https://www.unicef.org/innocenti/media/8181/file/UNICEF-Innocenti-Time-Using-Digital-Tech-Impact-on-Wellbeing-2017.pdf>.

6. L'identità digitale e il problema della costruzione della reputazione.

L'uso degli strumenti digitali porta alla costruzione di una identità digitale che — al netto dell'effettiva efficacia dell'esercizio del diritto all'oblio ⁽⁶²⁾ — può avere implicazioni a lungo termine, non sempre prevedibili.

Tecnicamente i confini dell'identità digitale sono tracciati dai profili di autenticazione e controllo all'accesso agli stessi, con livelli di sicurezza differenziati. Si pensi a tal proposito che i profili dei minori di età per l'erogazione dei servizi pubblici (dalla sanità, ai servizi educativi, alle misure a sostegno del nucleo familiare, etc.) sono attivati a mezzo di chiave crittografata a doppio livello di sicurezza nell'ambito delle identità digitali dei genitori ⁽⁶³⁾.

Per i profili non legati all'erogazione di prestazioni pubbliche, pertanto, la delimitazione degli accessi (ovvero il non ripudio dei dati sono legati a misure di crittografia di tipo basilare) come le *password*. A questo proposito i prestatori di servizi digitali adottano misure di sicurezza specifiche volte a proteggere la riservatezza e l'integrità dei profili introducendo regole di composizione delle parole chiave in modo che siano quanto più possibile difficili da ricostruire, ma anche su questo aspetto la diversa percezione della riservatezza, confidenzialità e integrità tra bambini, adolescenti e adulti deve poter costituire elemento di valutazione nell'elaborazione di linee guida e attività di formazione, al fine di poter garantire — anche per i più giovani — la tracciabilità e poter dare evidenza della paternità delle attività poste in essere nella dimensione digitale.

Sul piano tecnico, la normativa sulla strategia dei dati attribuisce agli operatori economici la responsabilità di valutare e introdurre misure di sicurezza e adattamenti per i profili dei minori di età, prevedendo — ad esempio — meccanismi di controllo degli accessi in favore del genitore, introducendo notifiche di richiesta di validazione di

⁽⁶²⁾ La de-indicizzazione sui motori di ricerca, per esempio, è considerata misura più efficace della richiesta di cancellazione degli *account*, G. FINOCCHIARO - O. POLLICINO, *Deindicizzazione: nuovi oneri per i motori di ricerca*, Ilsole24ore, 11 aprile 2022.

⁽⁶³⁾ L'AgID ha elaborato delle linee guida per consentire altresì l'acquisizione di spid per i bambini che abbiano compiuto i cinque anni, da utilizzare in via sperimentale: AGID, Determinazione n. 51 del 3 marzo 2022 - Adozione e applicazione delle "Linee guida operative per la fruizione dei servizi SPID da parte dei minori.

certe attività, laddove vi siano accessi al profilo del minore da dispositivi diversi da quelli generalmente utilizzati o addirittura previamente autorizzati all'uso, etc ⁽⁶⁴⁾.

Un ulteriore elemento di criticità nell'ambito della costruzione di una identità digitale è quello relativo alla reputazione ⁽⁶⁵⁾. Ciò vale direttamente allorché sia il minore a gestire in autonomia un profilo, sia con riferimento alle attività degli adulti, che il bambino subisce passivamente ⁽⁶⁶⁾.

Le linee guida diffuse da organizzazioni internazionali, anche in questo caso, contengono indicazioni legate alla necessità di mantenere il controllo delle informazioni condivise nello spazio digitale, nonché di riflettere in ottica prognostica rispetto al senso di vita privata e riservatezza — proprio e di terzi — che potrebbe essere minato in futuro dalla condotta dell'adulto che abbia messo in circolazione, in maniera permanente, una informazione riguardante la sfera intima e personale dell'interessato, che potrebbe anche non avere un profilo digitale su

⁽⁶⁴⁾ Si vedano gli standard IEEE illustrati nel capitolo precedente, IEEE, *Standard for an Age Appropriate Digital Services Framework Based on the 5Rights Principles for Children*, in IEEE Std 2089-2021, cit.

⁽⁶⁵⁾ Secondo l'agenzia per il digitale la reputazione digitale riguarda sia persone fisiche, che giuridiche, ed è costituita dalla “*percezione che gli utenti del web hanno di quello specifico soggetto*”, attraverso “*ogni comportamento e ogni notizia reperibile in rete [che] contribuiscono a formare l'idea che l'utente si crea e il giudizio che lo stesso esprime con riferimento ad una persona o ad un brand*”, a prescindere dall'accuratezza dell'informazione, ne derivano atteggiamenti di stima, fiducia, popolarità o viceversa innescare meccanismi di odio. Sulle criticità per i bambini anche in termini di pericolo di adescamento, si veda il rapporto di Save the Children, *Atlante dell'infanzia (a rischio) in Italia - Tempi digitali*, <https://s3.savethechildren.it/public/files/uploads/publicazioni/xiv-atlante-dellinfanzia-rischio-tempi-digitali.pdf> e quello Better Internet for Kids, *Classifying and responding to online risk to children*, 2023, che stabilisce la definisce “*as the information that can be found about an individual online. It becomes a matter of concern when harm occurs as the result of the way that a child is perceived in the digital environment*”. In dottrina A. RICCI, *La reputazione: dal concetto alle declinazioni*, Torino, 2019.

⁽⁶⁶⁾ T. LEAVER, *Balancing privacy: sharenting, intimate surveillance, and the right to be forgotten*, In: L. GREEN, D. HOLLOWAY, K. STEVENSON, T. LEAVER, L. HADDON (a cura di), *The Routledge Companion to Digital Media and Children*, London, UK: Routledge, 2020. pp. 235-44; G. OUVREIN, K. VERSWIJVEL, *Sharenting: parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management*, *Child Youth Serv Rev.* 2019 Apr; 99:319-27. doi: 10.1016/j.chilyouth.2019.02.011.

qualche piattaforma, ma essere comunque oggetto di contenuti condivisi da terzi ⁽⁶⁷⁾.

La letteratura identifica alcune conseguenze pregiudizievoli per la reputazione che nel bambino diventano più gravi essendo per maturità e lungimiranza ridotta meno percepibile il rischio sia in termini di serietà delle implicazioni che di occorrenza di situazioni, che possono variare dal mero fastidio a disagi e disturbi comportamentali. Si tratta di condotte relative alla pubblicazione di contenuti di cui, magari gli stessi autori si pentiranno in futuro: possono riguardare la propria persona o terzi, e anche in questo caso variare da mere leggerezze a condotte che istighino all'odio, violenza, discriminatorie o che minino l'incolumità della persona. Tali problematiche sono strettamente connesse, ad esempio, ai rischi di cyberbullismo o prestano il profilo ad essere oggetto di adescamenti o altre condotte illecite volte a ledere la sfera intima, personale e, talvolta, anche sessuale del minore. Rientrano nell'esempio anche attività del tutto ritenute innocue dall'agente, come le pratiche di *sharenting* da parte di familiari che, senza voler recare nocumento, possono abilitare accessi e usi inappropriati da parte di terzi, anche in buona fede ⁽⁶⁸⁾.

Anche in questo caso, la costruzione di identità digitali per i giovani deve essere accompagnata da una capillare campagna di sensibilizzazione, destinata sia ai bambini di diverse fasce di età che, soprattutto, a genitori e adulti di riferimento per consentire di trasmettere una attitudine a valutare le possibili implicazioni della condivisione nell'immediato, breve, e lungo periodo, attraverso una accurata conoscenza dei meccanismi di funzionamento dei sistemi informativi e delle possibili elaborazioni ⁽⁶⁹⁾.

L'ulteriore profilo di rischio legato all'associazione di contenuti a

⁽⁶⁷⁾ “L'immagine di mio figlio/figlia che sto per postare è privata e intima? Ha senso che sia resa pubblica? Mio figlio/a vorrebbe che condividessi pubblicamente quello che mi ha detto di lui/lei oggi la maestra? Tra 10 anni, sarà contento/a di trovare online questa immagine o video di sé? Sto condividendo una foto/video di mio figlio/a in una chat di gruppo, sono sicuro/a che non verrà scaricato da qualcuno e usato in altre chat?”, Save the Children, *ibidem*.

⁽⁶⁸⁾ P. FERRARA ET AL., *Online “Sharenting”: The Dangers of Posting Sensitive Information About Children on Social Media*, European Paediatric Association, Volume 257, 113322, June 2023, <https://doi.org/10.1016/j.jpeds.2023.01.002>

⁽⁶⁹⁾ OECD, *Children in the digital environment*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389?_ga=2.138548851.1597661473.1707343531-2141752145.1706178830.

identificativi è particolarmente frequente nei bambini in ragione della ridotta capacità di comprendere i pericoli cui consegue una maggiore esposizione a situazioni pregiudizievoli: il furto di identità o la frode, a seguito di tecniche di *hackeraggio*, spesso difficili da riconoscere per gli adulti e, ancor di più per i giovani, ovvero il furto di dati o la violazione della proprietà intellettuale, fino alle ipotesi di pirateria cui i giovani possono essere più esposti anche in ragione delle ridotte capienze patrimoniali ⁽⁷⁰⁾.

Attualmente nel nostro ordinamento sono state presentate due proposte di legge volte a disciplinare attraverso autorizzazione dell'Autorità della Concorrenza e del Mercato il fenomeno dei *baby-influencer*, estendendo di fatto le tutele proprie del diritto del lavoro. Nell'ambito delle iniziative si prevede da un lato, il diritto del ragazzo che abbia compiuto quattordici anni ad esercitare il c.d. oblio digitale, mentre che per le attività di *sharenting* sulle piattaforme *social*, nell'altra proposta si specifica che queste ultime debbano richiedere il consenso di entrambi i genitori, previa informativa specifica sui rischi connessi a tale condotta per i bambini ⁽⁷¹⁾.

Nella società della datificazione, infatti, chiunque può accedere a informazioni al livello globale e crearsi una percezione del tutto personale — anche se non necessariamente veritiera — che umanamente può poi rendere meno oggettiva una possibile valutazione vuoi per finalità di istruzione, o professionali, rendendo vulnerabile, di fatto, chiunque.

7. La prospettiva partecipativa nella dimensione digitale.

La dimensione partecipativa costituisce il vero valore innovativo dell'attuazione dei diritti fondamentali della persona nell'era digitale e, pertanto, tale principio deve trovare concreta applicazione anche verso i minori di età. Abbiamo fatto cenno al *favor* del legislatore europeo a costruire percorsi di condivisione dei processi decisionali con gli attori interessati: dalla adozione di codici di condotta nelle iniziative sulla

⁽⁷⁰⁾ Better for kids, *cit.*

⁽⁷¹⁾ La proposta di legge n. 1771 e n. 1800, Camera dei deputati, in materia di minori e Internet, con riferimento particolare all'accesso alle piattaforme e all'uso dell'immagine dei minori AA.C. 1217, 1771, 1800 e 1863, 18 giugno 2024, https://documenti.camera.it/leg19/dossier/pdf/TR0109.pdf?_1722466765385.

strategia dei dati, ai meccanismi di valutazione e mitigazione dei rischi, fino alla validazione dei risultati delle elaborazioni, la persona interessata è — sì — protetta, ma svolgendo un ruolo attivo nei meccanismi di tutela individuale e collettiva ⁽⁷²⁾.

Questo principio si manifesta in diversi scenari. In primo luogo, in caso esercizio dei diritti di cui agli artt. 15 e seguenti del GDPR, che attribuiscono un potere di controllo che perdura per tutto il ciclo del trattamento dei dati: il diritto all'accesso al flusso di informazioni (così come quello alla rettificazione) esprime un contributo proattivo alla verifica della gestione dei dati per la relativa corretta elaborazione ⁽⁷³⁾. Siffatto controllo è incentivato nell'ottica di condivisione e di creazione di spazi comuni di dati che siano riutilizzabili per finalità di interesse pubblico. In questo secondo scenario, si inserisce il meccanismo dell'altruismo dei dati, previsto dal Regolamento Europeo relativo alla governance europea dei dati ⁽⁷⁴⁾: si tratta di un esempio di partecipazione attiva alle opportunità della datificazione della società, basata sulla volontà del soggetto, che abilita la condivisione delle informazioni personali ad organizzazioni opportunamente registrate che, di fatto, agiscono come intermediari di dati senza scopo di lucro ⁽⁷⁵⁾.

Un'ulteriore espressione della compartecipazione ai processi decisionali si manifesta attraverso lo scambio di informazioni fra utente e macchina. Sia nel settore sanitario, che in quello educativo, come abbiamo visto, l'interazione tra il bambino e la soluzione tecnologica può costituire un momento di allenamento dei meccanismi di decisione

⁽⁷²⁾ G. LAZCOZ, P. DE HERT, *Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdicating responsibilities*, in *Computer & Law Security Review*, 2023, 50, 105833, 7-8.

⁽⁷³⁾ S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018.

⁽⁷⁴⁾ Regolamento Europeo del 30 maggio 2022, n. 868 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati). In dottrina: A. VIGORITO, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, MediaLaws, 2023, <https://www.medialaws.eu/rivista/sul-crinale-tra-data-altruism-e-social-scoring-esperienze-applicative-della-sequenza-dati-algoritmi-nel-nuovo-contesto-regolatorio-europeo/>, D. POLETTI, *Gli intermediari dei dati* (2022) 1 EJPLT, 45-56. doi: <https://doi.org/10.57230/EJPLT221DP>, G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di Diritto pubblico*, 2022, p. 975.

⁽⁷⁵⁾ J. RUOHONEN, S. MICKELSSON, *Reflections on the Data Governance Act*, DISO 2, 10 (2023). <https://doi.org/10.1007/s44206-023-00041-7>.

automatizzata, nonché di prestazione di un determinato servizio, cui segue un necessario processo di validazione umana, vuoi dal minore stesso, vuoi dall'adulto di riferimento ⁽⁷⁶⁾. Anche in questo caso, l'utente — indipendentemente dall'età — è parte integrante dei processi decisionali automatizzati. Per tale ragione, assume ancora più rilievo l'opinione circa l'usabilità e accettabilità della specifica soluzione, nonché l'identificazione di misure organizzative idonee per l'introduzione o l'implementazione in certi contesti.

Occorre, dunque, interrogarsi se (e fino a che punto) i menzionati diritti possano essere esercitati anche dai minori di età e, anzi, in ragione dell'abbassamento della soglia di cui all'art. 8 GDPR, e relative applicazioni nazionali, se sia possibile un'iniziativa autonoma dell'utente o meno.

Se nella dimensione fisica il diritto del minore ad esprimere la propria opinione e ad essere ascoltato ha trovato concreto riconoscimento prevalentemente in sede giurisdizionale ⁽⁷⁷⁾, nella dimensione digitale, è compito degli sviluppatori coinvolgere nella progettazione e sviluppo di nuove tecnologie processi di co-creazione, indirizzandoli in ragione dei bisogni, delle attitudini e delle caratteristiche dei gruppi di riferimento. Quattro sono i ruoli identificati per i bambini per considerarli parte di un processo di progettazione di una soluzione tecnologica: come utente, *tester*, informatore e *partner* a seconda delle dinamiche di potere con le figure professionali adulte ⁽⁷⁸⁾. Lo scopo è

(76) V. CHARISI, S. CHAUDRON, R. DI GIOIA, R. VUORIKARI, M. ESCOBAR-PLANAS, I. SANCHEZ, E. GOMEZ, *Artificial Intelligence and the Rights of the Child Towards an Integrated Agenda for Research and Policy*, cit.

(77) W. SCHRAMA, M. FREEMAN, N. TAYLOR, M. BRUNING (a cura di), *International Handbook on Child Participation in Family Law*, Cambridge-Antwerp-Chicago, 2021 per una applicazione in Italia, si veda il rapporto dell'Autorità Garante per l'infanzia e l'adolescenza, *Il diritto all'ascolto delle persone di minore età in sede giurisdizionale*, 2020, <https://www.garanteinfanzia.org/sites/default/files/ascolto-minorenni-procedimenti-giurisdizionali.pdf>.

(78) Per quanto riguarda la partecipazione a studi di carattere scientifico, ad esempio, si parla di partecipazione (1) contributiva, se la partecipazione all'osservazione di un fenomeno avviene attraverso la raccolta di dati; (2) collaborativa, cui si aggiunge alla contributiva il fatto che i partecipanti contribuiscano anche alla progettazione, interpretazione e diffusione dei risultati; (3) co-creazione, se vi è un rapporto reciproco di collaborazione sin dall'inizio del progetto scientifico; (4) contrattuale, se i partecipanti sono anche committenti della ricerca per ricevere certi risultati. A queste ipotesi collaborative si aggiunge quella di partecipazione indipendente di gruppi di movimenti di attivisti o cittadini non professionisti che promuovono certe analisi, per

quello di cambiare gli obiettivi, i processi e le unità di misura dei risultati per renderli “*child-friendly*”. Le modalità di ingaggio possono essere molteplici: da consultazioni pubbliche, a creazione di momenti di condivisione con specifici gruppi, questionari e interviste che possano fornire dati qualitativi e quantitativi sul ciclo di vita di un servizio o prodotto della società dell’informazione. Ciò vale per tutte le fasi: dalla progettazione, all’uso, all’eventuale attività di reclamo in caso di contenuti o attività considerate improprie o inidonee per il singolo, etc. Da questo punto di vista, l’obbligo per le piattaforme digitali di introdurre sistemi di segnalazione e reclamo — che sono validi anche (e soprattutto) per i servizi destinati ai minori di età — costituisce una forma di promozione della partecipazione attiva del minore a contribuire ad un ambiente digitale più sicuro per sé, e per gli altri utenti ⁽⁷⁹⁾.

Introdurre nei processi decisionali anche al livello più granulare meccanismi di compartecipazione dei minori di età di varia natura, inclusa la mediazione e rappresentanza di associazioni di professionisti capaci di raccogliere dati e riassumere le diverse voci dei bambini su una determinata questione, facilita l’opportunità di veicolare il relativo punto di vista anche di fronte ai tavoli di discussione al livello politico-istituzionale, affinché l’organizzazione dei servizi e dei prodotti sia resa a portata del bambino.

8. La responsabilizzazione delle istituzioni e degli operatori economici.

La costruzione di un ecosistema digitale umano-centrico richiede notevoli investimenti, sia per le istituzioni, che per le organizzazioni private, affinché le procedure di sviluppo ed erogazione di servizi e

un approfondimento B.V. CARBALLIDO, J. DÍEZ-PALOMAR, C. GARCIA-YESTE, ET AL, *The effects of children’s participation and co-creation in science*, Humanit Soc Sci Commun 11, 3 (2024), <https://doi.org/10.1057/s41599-023-02473-5>. Con riferimento ai bambini, S. MATHIYAZHAGAN, K. LA FORS, *Children’s right to participation in AI: Exploring transnational co-creative approaches to foster child-inclusive AI policy and practice*. Info. Pol. 28, 1 (2023), 141-153, <https://doi.org/10.3233/IP-229014>.

⁽⁷⁹⁾ S. MATHIYAZHAGAN, K. LA FORS, *Children’s right to participation in AI: Exploring transnational co-creative approaches to foster child-inclusive AI policy and practice*, cit.

prodotti siano conformi ai valori espressi nella Carta dei Diritti Fondamentali dell'UE e, nel nostro caso, all'architettura costituzionale ⁽⁸⁰⁾.

Da questo punto di vista, l'assenza di una normativa interna che raccolga le disposizioni di settore per promuovere un ambiente digitale alla portata dei bambini, alla stregua della risoluzione brasiliana commentata nei capitoli precedenti, impone di strutturare valutazioni del rischio che siano ritagliate ai bisogni e ai pericoli che, di volta in volta, emergono nello sviluppo e utilizzo di tecnologie. Si manifesta così lo stretto rapporto fra responsabilizzazione e responsabilità che vede la *compliance* etico-giuridica del singolo operatore, come strumento di prevenzione non solo del rischio in ottica utente-centrica, ma anche di prevenzione rispetto alle ipotesi patologiche che potrebbero determinare condanne risarcitorie e sanzionatorie.

Sulla base del principio di responsabilizzazione, istituzioni e operatori devono contribuire non solo ad evitare pregiudizi, ma anche a costruire processi virtuosi che tengano conto della necessità di promuovere, oltre che di proteggere, le prerogative dei minori di età. Ciò al fine di addivenire in maniera effettiva alla costruzione di una dimensione digitale alla portata di tutti i bambini, ove i diritti, declinati attraverso formule diverse, ovvero attuati con strumenti di diverso rango ed efficacia, possano aspirare ad avere un riconoscimento universale anche nella società dell'informazione.

Per queste ragioni, i requisiti di robustezza, gli *standard* tecnici e le certificazioni — che sono propri della sfera tecnologica per uniformare le valutazioni delle prestazioni rispetto ai requisiti di sicurezza, affidabilità - possono costituire l'occasione per identificare procedure e misure organizzative, altrettanto condivise, che guidino gli operatori economici nel dimostrare di adempiere con diligenza e professionalità agli obblighi imposti dalla normativa di settore. Le singole attività di *compliance* a queste misure, infatti, devono prestare attenzione a quei profili di criticità legati alla ridotta capacità di discernimento, al fine di fornire loro strumenti, opportunità di formazione, e modelli, per riflettere sui pericoli da evitare e sugli spazi per attuare quella soluzione, che sia in grado di cogliere il miglior interesse per quella tipologia di utente e, allo stesso tempo, di rappresentare le diversità in ottica inclusiva.

(80) EU COMMISSION, *Digital4Development: mainstreaming digital technologies and services into EU Development Policy*, Brussels, 2.5.2017 SWD(2017) 157 final.

In primo luogo, occorre investire nella mappatura e aggiornamento delle buone prassi e in percorsi formativi per facilitarne l'implementazione nei singoli scenari. Dopodiché, serve introdurre degli incentivi affinché la conformità e l'adesione spontanea possano essere effettivi. A questo proposito, si potrebbe trattare di sgravi fiscali, ovvero di *bonus* per il reclutamento di figure specializzate, o per l'introduzione di percorsi di formazione per il personale dedicato alle valutazioni di impatto, o — ancora — di sovvenzioni per l'avvio di consultazioni nei processi di progettazione di nuove soluzioni con bambini e adulti di riferimento.

8.1. (Segue). *La responsabilizzazione degli adulti e delle comunità di riferimento per il minore.*

Nell'allocazione di ruoli e responsabilità nella società dell'informazione gli adulti di riferimento, che non nutrono responsabilità *ex lege* verso il singolo bambino, possono contribuire alle sfide della datificazione attraverso una responsabilizzazione delle condotte proprie attive e omissive.

In particolare, con riferimento all'esposizione di informazioni che riguardano i bambini, un adulto — consapevole della facilità con cui un flusso di dati possa essere abilitato e condiviso e riutilizzato, con la conseguente rapida perdita del controllo sulle informazioni — sarà più sensibile a evitare di abilitare senza giustificato motivo, oltre che senza autorizzazione, immagini, video, audio etc. che riguardino i bambini ⁽⁸¹⁾.

Si tratta in questo contesto di un cambiamento culturale, che deve essere indirizzato con una pluralità di interventi e in maniera capillare anche e soprattutto tra gli adulti. Infatti, la condivisione di contenuti, anche relativi alla propria vita privata nella dimensione digitale, è espressione di una serie complessa di attitudini che sono legate agli stati d'animo e alla ricerca di benessere ⁽⁸²⁾, non associabili né ad un più

⁽⁸¹⁾ Le campagne di sensibilizzazione delle autorità garanti per la protezione dei dati personali sono esplicite, necessiterebbero di una maggiore diffusione, si veda ad esempio quella relativa alle buone prassi in vacanza, che raccomanda di evitare di “postare” foto sui social network che rappresentino minori di età, e allo stesso tempo forniscono indicazioni sui relativi rischi, in modo da poter estendere le riflessioni anche agli usi quotidiani: <https://www.garanteprivacy.it/temi/estate>.

⁽⁸²⁾ D. JOYE, M. SAPIN, C. WOLF, *Measuring Social Networks and Social Resources. An Exploratory Study around the World*. Köln, Germany, 2019.

basso livello di istruzione, né ad una specifica condizione socio-economica. Lo spazio digitale decostruisce le esperienze individuali, conferendo loro nuovi significati attraverso la condivisione e senso di comunità che ne deriva.

A fronte della datificazione della società, infatti, la condizione di vulnerabilità — comune a tutti gli utenti — non riguarda solo la prospettiva passiva, ovvero il fatto di essere soggetti a perdere il controllo delle informazioni o a essere profilati e classificati con implicazioni indirette, difficilmente prevedibili, ma concerne anche — e soprattutto — la posizione di debolezza rispetto ai poteri privati, che in maniera sempre più pervasiva ⁽⁸³⁾, esercita pressioni rispetto alla costruzione di identità digitali nell'ambito delle quali l'individuo realizza la propria personalità.

In ottica solidale, pertanto, responsabilizzare le comunità di riferimento significa, anche in questo caso, come visto per gli operatori economici, facilitare momenti di confronto e sensibilizzazione affinché la cittadinanza, sia dapprima resa edotta, attraverso iniziative di alfabetizzazione digitale ed educazione, e possa poi formarsi una coscienza digitale condivisa e ritagliata alla realtà comune.

Infine, occorrono investimenti per poter mettere in condivisione risorse digitali volte a facilitare non solo l'uso di servizi di comunicazione legati a *smartphone* o *tablet*, come piattaforme di messaggistica o *social network*, ma anche lo sviluppo di competenze per la diffusione di una cultura digitale capace di creare contenuti, strumenti utili per la vita quotidiana, e chiavi interpretative per nozioni di base — seppur tecniche — al fine di comprendere i meccanismi di decisione automatizzata e prendere determinazioni consapevoli riguardo all'uso (o meno) di determinati prodotti o servizi ⁽⁸⁴⁾.

9. Costruire una dimensione digitale assieme a (e alla portata di) bambini e adolescenti...

Nei paragrafi precedenti abbiamo declinato i diritti dei bambini

⁽⁸³⁾ P. STANZIONE, *Data Protection and Vulnerability*, 2020, Eur. J. Privacy L. & Tech. 9.

⁽⁸⁴⁾ CONIMPRESASOCIALE, *L'uso consapevole di internet e le competenze digitali nelle scuole*, 30 gennaio 2024, <https://www.conibambini.org/osservatorio/luso-consapevole-di-internet-e-le-competenze-digitali-nelle-scuole/>.

nella dimensione digitale, formulando possibili raccomandazioni, volte ad attuare il principio di perseguimento degli interessi superiori del fanciullo in scenari di vita quotidiana. Abbiamo fatto emergere i profili di tensione derivanti dai rischi e dalle opportunità, al fine di cogliere possibili chiavi di lettura per orientare l'interprete nell'identificazione di un corretto bilanciamento tra gli interessi emergenti in ottica di perseguimento del benessere del minore di età.

Abbiamo, in particolare, per ciascun profilo esplicitato la possibile distribuzione di ruoli e responsabilità affinché adulti di riferimento, istituzioni e organizzazioni private possano contribuire a disegnare una dimensione digitale, non solo sicura e affidabile per tutti, ma attenta alle esigenze di tutela dei diritti dei minori di età. Abbiamo dunque osservato come, in ragione dei bisogni e del grado di maturità, sia opportuno indirizzare gli interventi di politica del diritto, distinguendo gli utenti e il loro sviluppo psicofisico in almeno due macro-categorie: i bambini, il cui rapporto con le tecnologie deve essere prevalentemente accompagnato e in ogni caso supervisionato dagli adulti, e gli adolescenti che gradualmente acquisiscono maggiore indipendenza nel fruire di prodotti e servizi della società dell'informazione cui occorre riconoscere progressivamente spazi di autonomia decisionale e operativa.

Abbiamo evidenziato perciò la necessità di introdurre incentivi, affinché si diffonda una capillare cultura alla digitalizzazione e dei sistemi di IA nella società civile, che riduca le fonti di esposizione ai rischi, attraverso un più responsabile uso delle tecnologie, e che promuova l'accessibilità alle risorse e alle infrastrutture, assicurando, allo stesso tempo, che le barriere all'inclusività non siano alimentate né dallo sfruttamento di vulnerabilità note da parte di operatori o di altri utenti, né da quelle ignote, che potrebbero emergere nel tempo dall'uso improprio delle soluzioni digitali e dall'impatto dell'evoluzione delle tecnologie.

Al contempo, occorre strutturare le premesse perché l'ambiente digitale a misura di bambino e adolescente possa essere mantenuto — e non solo riconosciuto — come tale a prescindere dai confini geografici o dalle giurisdizioni, sfruttando il carattere universale sia dei diritti dell'infanzia e dell'adolescenza, da un lato, sia degli *standard* tecnici, dall'altro ⁽⁸⁵⁾. Con riferimento a quest'ultimo profilo, abbiamo osser-

(85) C. LI, B. PALANISAMY, *Privacy in Internet of Things: From Principles to Technologies*, in IEEE Internet of Things Journal, 2019, p. 488 s.

vato come la circolazione e l'allineamento delle misure di salvaguardia di tipo tecnico, peraltro, portino alla definizione e condivisione di buone prassi anche di tipo organizzativo, per facilitare l'adeguamento da parte degli operatori economici al gran numero di obblighi imposti dalle diverse normative di settore. Essendo l'affidabilità e sicurezza dello spazio digitale e delle tecnologie affidate alla percezione dei rischi emergenti in sede di obblighi di valutazione e di *due diligence* da parte degli operatori economici, una spontanea proceduralizzazione delle attività di valutazione di impatto, fondata sul carattere universale delle premesse (*i.e.* i diritti fondamentali riconosciuti nella CRC e declinati nella dimensione digitale), dell'oggetto di valutazione (*i.e.* i rischi con conseguente esposizione a compromissione e lesione dei diritti determinando pregiudizi per la sicurezza, incolumità e benessere), delle risposte (*i.e.* come misure tecniche di sicurezza) e del parametro orientativo (*i.e.* il perseguimento degli interessi superiori dei bambini e degli adolescenti), appare un contributo valorizzabile in termini di *soft law* anche attraverso forme di autoregolamentazione espresse in codici di condotta e certificazioni cui gli stessi operatori potranno aderire ⁽⁸⁶⁾, ovvero attraverso *policy* e raccomandazioni da utilizzarsi in sede interpretativa dalle autorità competenti in materia ⁽⁸⁷⁾.

Se la valutazione qualitativa e quantitativa dei rischi e delle relative misure di mitigazione assume — al pari dei diritti fondamentali enucleati nella CRC — un ruolo di primo ordine, è altrettanto vero che l'approccio responsabile può formarsi e mantenersi solo accompagnando un eventuale intervento normativo di settore che incentivi e in certi termini imponga una diffusione di competenze e abilità comuni, almeno ad un livello base, che possa rendere l'educazione digitale una componente essenziale del vivere civile. Ciò non solo per le nuove

⁽⁸⁶⁾ Nel corso della revisione delle bozze è stata presentata la seconda versione del Second Draft General-Purpose AI Code of Practice volto ad assicurare che i fornitori di modelli di IA di tipo generativo possano effettivamente rispettare i propri obblighi ai sensi del Regolamento UE sull'IA, dove si sottolinea la necessità di bilanciare impegni chiari con la flessibilità di adattamento resa necessaria dalla quotidiana evoluzione della tecnologia, Second Draft General-Purpose AI Code of Practice, disponibile <https://ec.europa.eu/newsroom/dae/redirection/document/111374>.

⁽⁸⁷⁾ Nel corso della revisione delle bozze del presente volume sono state, ad esempio, pubblicate le posizioni dell'EDPB sui modelli basati sull'IA: EDPB, *Opinion on AI models: GDPR principles support responsible AI*, 18 dicembre 2024, disponibile qui https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en.

generazioni, ma anche per gli adulti che devono poter acquisire le idonee conoscenze e abilità per assumere ruoli di supervisione e accompagnamento, oltre che acquisire quegli strumenti conoscitivi necessari per utilizzare essi stessi in maniera responsabile lo spazio digitale e le tecnologie, nonché trasmettere il proprio bagaglio di conoscenze attraverso i compiti di cura, istruzione ed educazione dei giovani utenti.

Per tale ragione, la proposta di introdurre un “*patentino digitale*”, quale percorso formativo e di rafforzamento di competenze certificabili e riconoscibili dagli operatori economici diventa un tassello fondamentale dell’architettura portante per lo sviluppo di dimensione digitale sicura, affidabile e a misura di bambini, da accompagnarsi, in ogni caso, sia alle iniziative già in discussione — e rivolte agli adulti — per l’alfabetizzazione digitale dei cittadini, sia al sistema di tutele civili, amministrative e penali che si pongono in funzione deterrente e punitiva rispetto al perpetrare usi impropri e abusi che configurino condotte illecite nello spazio digitale o esponano i minori di età a rischi o pericoli.

I diversi moduli del percorso di alfabetizzazione dovrebbero contenere — con linguaggio semplice, chiaro e con un livello di dettaglio commisurato all’età (e dunque alle capacità di discernimento) dei discenti — tematiche legate ai dati personali e alla *privacy*, alla cybersicurezza, nonché alle questioni etico-giuridiche emergenti dall’interazione con le tecnologie: dal funzionamento alla spiegabilità dei processi automatizzati, al concetto di *bias*, al ruolo del controllo e partecipazione umana nella progettazione, *test* e — soprattutto — nella validazione dei risultati.

Il filo rosso tra i diversi livelli dovrebbe essere quello di coniugare conoscenze specifiche con i relativi diritti esercitabili da parte dell’utente con la presa di coscienza dei comportamenti che, invece, costituiscono condotte irresponsabili, se non addirittura illecite, ciò sia in termini di soggetto agente, che di vittima. Tra gli obiettivi formativi, così facendo, si potrebbero allenare in misura sempre più accurata e specifica quelle abilità — proprie della capacità di discernimento — che consentono di prevenire i rischi o di prendere contromisure efficaci in caso di manifestarsi di pericoli immediati, in modo da evitare pregiudizi.

In questo modo, si trasmetterebbe il messaggio per cui — al pari della vicenda della circolazione stradale — avendo lo spazio digitale e l’innovazione tecnologica regole ben precise per evitare o limitare

pericoli per l'incolumità e la sicurezza propria e altrui, occorre verificare la sussistenza di competenze di base, prima di accedervi. Tali competenze, acquisibili mediante un percorso di formazione e accertate a mezzo di certificazione (come abbiamo visto anche sulla base dei possibili schemi in discussione al livello UE, purché adattati alle metodologie di insegnamento riconosciute come efficaci per le relative fasce di età) dovranno comprendere elementi teorici (ad esempio una approfondita conoscenza dello spazio e delle condizioni di accesso — per rimanere nella metafora dei segnali stradali — e dei meccanismi di funzionamento delle applicazioni e soluzioni utilizzate — *mutatis mutandis* delle caratteristiche dei veicoli e del loro funzionamento —) che pratiche, al fine di esercitare capacità di risoluzione di problemi e di affrontare eventuali pericoli in ragione delle diverse tipologie di utenti che possono incontrare.

In misura complementare al sistema di tutele per le vittime di illeciti civili o penali, si tratterà, dunque, di creare meccanismi di coordinamento e cooperazione con gli obblighi di *due diligence* previsti per i prestatori di servizi digitali, di conformità per gli sviluppatori di sistemi basati sull'IA e per i titolari di trattamento per favorire l'accesso con gradi di autonomia progressivamente diversificati per coloro che avranno ottenuto il c.d. "patentino digitale". Per contro, sarà necessario limitare la gestione dei profili senza un ruolo attivo di supervisione da parte dell'esercente le responsabilità genitoriali laddove l'utente non abbia ottenuto la certificazione di alfabetizzazione, nonostante il compimento del quattordicesimo anno di età.

Questo approccio appare facilmente implementabile attraverso la collaborazione dei sistemi educativi, delle autorità garanti ed esportabile in tutti i sistemi analizzati, declinando le conseguenze sulla base dell'età minima di riferimento per la normativa nazionale, ovvero della valutazione della capacità di discernimento dell'utente e del ruolo eventualmente più dettagliato dei genitori rispetto agli obblighi degli operatori economici di introdurre meccanismi di protezione *by default* da eventualmente disinnescare.

9.1. (Segue). ...e le considerazioni di sistema.

Le proposte di legge attualmente in discussione nel nostro ordinamento non sembrano cogliere i profili illustrati nel paragrafo precedente, riguardando prevalentemente il rapporto dei minori di età con i *social media* e, in quest'ottica, riservandosi di proporre in alcuni casi di

aumentare di un anno la soglia per esprimere consenso valido al trattamento dei dati personali per i servizi della società dell'informazione, associando obblighi di introduzione di sistemi di verifica dell'età dell'utente per i prestatori di servizi digitali; mentre altre disposizioni mirano ad introdurre misure per segnalare abusi (ad esempio un numero di emergenza); ed altre ancora mirano a rendere inefficaci, mediante nullità, i contratti digitali conclusi da minori di età; altre ancora regolamentano il fenomeno dei *baby influencer* stabilendo obblighi di depositi dei guadagni in conti dedicati ⁽⁸⁸⁾. Tutte le iniziative attualmente in discussione in Parlamento, tuttavia, appaiono carenti rispetto ai profili educativi che, invece, si ritengono fondamentali per poter rendere efficaci gli obblighi di protezione che il legislatore europeo ha già previsto e normato attraverso l'imposizione di obblighi di effettuare valutazioni di impatto da parte di titolari del trattamento, prestatori di servizi digitali, sviluppatori, distributori e *deployer* di sistemi basati sull'IA. Come osservato, infatti, la prescrizione di occuparsi della protezione dei diritti fondamentali dei bambini è presente in tutti e tre i Regolamenti rilevanti (GDPR, DSA, IA) per la disciplina di uno spazio digitale e di tecnologie affidabili.

Ciò che potrebbe fare la differenza nel breve periodo, invero, è l'adozione di un provvedimento congiunto delle autorità garanti coinvolte (nella specie l'autorità garante per la protezione dei dati con funzioni anche di sorveglianza in materia di intelligenza artificiale e il coordinatore dei servizi digitali), al fine di dare indicazioni metodologiche per affrontare le valutazioni di impatto, affinché proteggano, lasciando spazio alla promozione di misure per la realizzazione della persona nello spazio digitale, a partire dagli effetti dell'ottenimento del "*patentino digitale*", quest'ultimo necessariamente da regolamentare con fonte di rango primario.

Le considerazioni di politica di diritto possono essere sintetizzate in cinque punti che dovrebbero poter indirizzare le proposte di riforma in ottica di costituire una cittadinanza digitale a partire dai giovani utenti, più responsabili non in quanto precocemente esposti all'uso di sistemi e tecnologie, ma perché formati e stimolati nello sviluppo di competenze specifiche e consapevolezza che — a cascata — li rendano

⁽⁸⁸⁾ Camera dei deputati, in materia di minori e Internet, con riferimento particolare all'accesso alle piattaforme e all'uso dell'immagine dei minori AA.C. 1217, 1771, 1800 e 1863, 18 giugno 2024, *cit.*

fruitori e consumatori della società dell'informazione progressivamente più autonomi. In particolare:

1. *Bisogni ed esigenze diversificati a seconda delle fasce di età degli utenti e del livello di educazione digitale.*

La già infelice formula “minore di età”, che appare sminuire la persona che non abbia compiuto gli anni diciotto come portatrice di interessi e di diritti fondamentali si presta a ulteriori profili di criticità nella dimensione digitale, laddove, come è emerso nelle pagine precedenti, non sia più efficace nemmeno per indicare una categoria omogenea di soggetti vulnerabili ⁽⁸⁹⁾.

Per quanto osservato, le valutazioni di impatto dovrebbero analizzare su piani diversi rischi, pericoli e relative misure di mitigazione, a seconda che l'utente sia bambino o adolescente e in ragione del livello di educazione digitale certificato a mezzo del proposto schema di “patentino digitale”.

2. *Allineamento della capacità di esprimere consenso valido a fini del trattamento dei dati personali, adesione a termini e condizioni contrattuali.*

Potrebbero essere messi a disposizione modelli di termini e condizioni d'uso, in ragione delle funzionalità del servizio digitale o del prodotto tecnologico, che stabiliscano piani ben definiti di consenso esprimibile dal minore e dall'adulto che eserciti le responsabilità genitoriali, distinguendo le condizioni per quello utile ai fini dell'adesione al servizio e quello necessario per eventuali trattamenti di dati ulteriori rispetto a quelli dovuti per l'esecuzione del contratto (altrimenti processabili ai sensi dell'art. 6, lett. b) GDPR).

La norma di rango primario sull'introduzione del “patentino digitale” potrebbe prevedere quale effetto della certificazione un allineamento dell'età per i fini di cui all'art. 2 *quinqüies* del Codice Privacy per l'adesione a servizi che siano destinati ai minori di età.

3. *Accesso a servizi digitali e tecnologie destinati anche agli adulti.*

Per i servizi, invece, destinati anche a utenti adulti, l'adesione

⁽⁸⁹⁾ Sarebbe auspicabile da questo punto di vista sostituire il termine “minore” nella normativa codicistica con bambini e adolescenti, alla stregua di quanto avvenuto con la l. n. 54/2006 tra potestà e responsabilità genitoriale: F.D. BUSNELLI, *Capacità ed incapacità di agire del minore*, cit.; F. GIARDINA, *La condizione giuridica del minore*, cit.

dell'adolescente munito di “*patentino digitale*” potrebbe essere subordinata all'introduzione *by default* di misure di protezione, suscettibili di essere disabilitate dal legale rappresentante o su richiesta dell'utente previo consenso del primo. Si potrebbe trattare di meccanismi che, come visto in alcuni sistemi che hanno sviluppato indicazioni pratiche come nel Regno Unito o in alcune legislazioni USA o in India ⁽⁹⁰⁾, blocchino la possibilità di profilare per finalità di *marketing*, ricercare contenuti e contattare da parte di profili gestiti da utenti adulti, rendere visibili e disponibili contenuti che possano essere considerati illeciti, che istighino alla violenza, discriminazione o, più in generale, non siano considerati appropriati per soggetti minorenni. Potrebbero, altresì, essere soggetti allo stesso regime contenuti e interfacce, che inducano e incentivino alla permanenza *online*, sulla base di attività di reportistica che possa essere trasmessa al genitore a fini di monitoraggio degli impatti dei servizi o dei prodotti sui figli.

L'adesione da parte di bambini, invece, dovrebbe essere accompagnata da un adulto e meccanismi di verifica della effettiva comprensione di genitori nell'utilizzo dei servizi e prodotti dovrebbero poter essere introdotti e funzionare *by design* e *by default* dai prestatori dei servizi e dai *deployer* delle tecnologie, come suggerito nel sistema cinese ⁽⁹¹⁾.

L'opzione di vietare l'uso di *social media* promossa da alcune iniziative legislative osservate nei capitoli precedenti (ad es. da alcuni stati USA, dall'Australia, e, più di recente in Spagna), seppur con caratteristiche diverse, non appare perseguibile senza ricadute drastiche sulla formazione di una cittadinanza digitale e consapevole.

Non si tratta, come abbiamo dimostrato, di aver raggiunto una certa età anagrafica, ma di aver rafforzato competenze e conoscenze per poter prevenire l'esposizione a rischi e, nella denegata ipotesi, di trovarsi in situazioni di pericolo, saper adottare misure idonee per evitare pregiudizi.

4. *Profili di responsabilità.*

La normativa che definisce gli effetti giuridici del “*patentino digitale*” non potrà esimersi dal prendere in considerazione le ricadute sui paradigmi di responsabilità. Abbiamo osservato come a una maggiore (e in tal caso certificata) autonomia decisionale debba corrispon-

⁽⁹⁰⁾ *Supra*, Cap. 1.

⁽⁹¹⁾ *Supra*, Cap. 2.

dere una altrettanto adeguata responsabilizzazione, che già nel sistema penale si riflette con la punibilità del soggetto che abbia compiuto gli anni quattordici. Orbene, sul piano civilistico ciò che rileva è senz'altro la garanzia che la vittima di un illecito possa trovare ristoro attraverso un risarcimento del danno, motivo per cui è il genitore — presumibilmente con un patrimonio più capiente rispetto al minore — che potrà rispondere economicamente del fatto del terzo ai sensi dell'art. 2048 c.c. Sul punto abbiamo evidenziato sia l'opportunità di prevedere possibili contemperamenti attraverso, ad esempio, l'introduzione di meccanismi di solidarietà e responsabilità sulla scia di quelli previsti dalla normativa in materia di responsabilità da circolazione stradale tra utente e proprietario del veicolo da adattarsi alla dimensione digitale: considerato che per i ciclomotori è richiesta l'assicurazione obbligatoria, come condizione per poter circolare su strada, potrebbe essere associato al patentino del minore di età anche una forma di assicurazione obbligatoria per la fruizione di (almeno certe) piattaforme digitali da parte di soggetti minori di età. Criterio discriminante in tale scenario potrebbe essere quello di combinare sulle criticità per i minori di età raccolti nei diversi sistemi: ad esempio nell'UE si potrebbero prendere in considerazione quei servizi digitali, che già nella prima fase di implementazione del nuovo Regolamento abbiano manifestato criticità rispetto alla tutela dei diritti fondamentali dei minori (ad esempio per *Very Large Online Platforms* collegate a servizi di *social network*), oppure quelle commerciali che potrebbero impattare sui profili patrimoniali del nucleo familiare (oltre che del minore di età).

5. *Misure di monitoraggio rispetto agli effetti sul benessere psicofisico degli utenti.*

Tra i rischi associati all'uso di servizi della società dell'informazione e delle nuove tecnologie abbiamo elencato la possibilità di sviluppare disturbi comportamentali e dipendenze, osservando come vi siano timori circa un'eccessiva standardizzazione del pensiero critico e una conseguente riduzione della stimolazione dei meccanismi di creatività del singolo individuo dovuti all'uso di nuove tecnologie sempre più sofisticate e applicate ai processi di apprendimento, alle arti e alle industrie creative. Del pari, abbiamo analizzato le potenzialità dell'uso delle tecnologie in termini di riduzione delle disuguaglianze a fronte di pari opportunità di accesso alle risorse.

Alla luce di queste considerazioni, appare utile poter introdurre dei meccanismi di monitoraggio rispetto agli andamenti che possono emer-

gere nel lungo periodo al fine di valutare l'efficacia delle misure di protezione (in sinergia con gli obblighi di reportistica degli operatori economici) e di quelle di promozione e potenziamento delle opportunità ⁽⁹²⁾.

In questa prospettiva, così come la patente di guida richiede forme di rinnovo che includono valutazioni sull'idoneità psicofisica, potrebbe valer la pena — quanto meno su base volontaria — avviare anche un programma di monitoraggio rispetto alle attitudini e ricadute sulla qualità della vita e sui comportamenti degli utenti. Ciò al fine di coinvolgere direttamente la generazione di primi patentati digitali, anche una volta raggiunta la maggiore età, e quelle successive, per comprendere l'impatto del meccanismo introdotto in un lasso di tempo capace di fornire una panoramica idonea per valutare interventi di aggiornamento e miglioramento e garantire la sostenibilità e il mantenimento virtuoso dell'investimento per una società dell'informazione e innovazione tecnologica a portata di bambini e adolescenti, ormai (già) giovani adulti ⁽⁹³⁾.

9.2. *La declinazione dei cc.dd. best interests of the child e gli spazi di "adattamento".*

Una volta indirizzati i profili di consistenza che renderebbero il sistema di tutele coerente non solo con l'assetto normativo esistente, ma anche con le esigenze emerse dall'analisi comparatistica, la riflessione appare sufficientemente matura per poter declinare il principio dell'interesse superiore del fanciullo rispetto alle caratteristiche di un rinnovato paradigma di protezione e tutela di bambini e adolescenti nella dimensione digitale.

Nel nostro percorso, infatti, abbiamo dapprima proceduto a "*de-terrorializzare il diritto*" ⁽⁹⁴⁾ mettendo assieme esperienze nazionali e

⁽⁹²⁾ Anche in ragione del fatto che "*la tecnica modifica il nostro modo di essere nel mondo e l'attuale è la prima generazione dove l'esperienza dei padri non può passare ai figli. Perché i padri sono vissuti in un mondo reale mentre i ragazzi vivono in un mondo virtuale*" U. GALIMBERTI, intervista del 23.04.2019, Il Dubbio.

⁽⁹³⁾ Comité de expertos para la creación de entornos digitales seguros para la infancia y la juventud, *Informe del comité de personas expertas para el desarrollo de un entorno digital seguro para la juventud e infancia*, cit.

⁽⁹⁴⁾ M.R. FERRARESE, *Globalizzazione, comparazione e il ruolo dei giuristi privati: verso un nuovo formante giuridico?*, in AA.VV., L. ANTONIOLLI, F. CORTESE, E. IORATTI, B. MARCHESE (a cura di), *Trento e la comparazione giuridica: voci, esperienze, riflessioni: dalla testimonianza di Rodolfo Sacco e Mauro Cappelletti*, 2024, p. 81 dove richiama il pensiero di Zumbansen che ha definito il diritto comparato come diritto transnazionale

sopranazionali di diversa natura. Complice — poi — il proposito di disciplinare fenomeni globali, come la datificazione della società e l'innovazione tecnologica, abbiamo interpretato gli interventi normativi e le iniziative di autoregolazione alla luce dei rischi propri di coloro che — per ragioni formalmente anagrafiche, ma sostanzialmente legate alla limitata, seppur fisiologicamente crescente, capacità di discernimento — appaiono, più di altri, utenti vulnerabili rispetto ai servizi e ai prodotti digitali. Abbiamo sin qui fornito risposte ad esigenze, altrettanto transnazionali, condivise e comuni, di protezione e promozione dei diritti fondamentali dei minori di età nella società dell'informazione, osservando una certa “*porosità tra diversi sistemi giuridici*” ⁽⁹⁵⁾ appartenenti a più famiglie giuridiche, nonché rappresentanti stadi differenti di regolazione della pluralità di settori di cui si compone la c.d. *data economy*.

A questo punto occorre tirare le fila operative e descrivere il risultato delle analisi condotte, delineando le caratteristiche del paradigma ⁽⁹⁶⁾ di protezione e promozione dei minori di età nella dimensione digitale, che siano frutto delle prassi condivise (*common core*) e di quelle più virtuose (*better rule*) ⁽⁹⁷⁾, capace di rispondere alle esigenze

e collega tale caratteristica altresì al ruolo della privatizzazione e professionalizzazione dell'iniziativa regolatoria. La riflessione appare calzante anche per la società dell'informazione che — come abbiamo osservato nei capitoli precedenti — grazie alla combinazione di istanze di *compliance*, le esigenze di standardizzazione soddisfatte dalla comunità scientifico-tecnologica di riferimento hanno estremamente influenzato il processo regolatorio.

⁽⁹⁵⁾ *Ibidem*.

⁽⁹⁶⁾ “*Il compito dell'interprete non è quello di accertare la crisi delle categorie, così contribuendo alla loro demolizione; bensì è quello — più difficile — di ridisegnarne il contenuto e i confini alla luce del nuovo, fino al punto di proporre di nuove, quando i fenomeni — per la loro consistenza, per la loro originalità e per la loro importanza — meritano la confezione di una categoria del tutto nuova (di matrice normativa, giurisprudenziale o dottrinale che sia)*”, così A.M. BENEDETTI, *Contratto e categorie: un paradigma, più discipline*, in *Pactum*, 2022, p. 21. La riflessione sulla crisi delle categorie di diritto privato è un tema dibattuto in dottrina, come nota F.D. BUSNELLI, *Quale futuro per le categorie del diritto civile?*, in *Riv. dir. civ.*, 2015, 5 ss. Si vedano anche G. ALPA, *Giuristi e interpretazioni. Il ruolo del diritto nella società postmoderna*, Genova, 2017, N. LIPARI, *Le categorie del diritto civile*, Giuffrè, 2013; R. SACCO, *Il fatto, l'atto, il negozio*, in *Trattato di diritto civile*, diretto da Sacco, Utet, 2005; A. GENTILI, *Crisi delle categorie e crisi degli interpreti*, in *Riv. dir. civ.*, 2021, 633 ss.

⁽⁹⁷⁾ Per la ricostruzione di principi applicabili in materia di tutela dei minori di età e di relazioni familiari attraverso la combinazione di elementi di *common core* e di *better rule*, si vedano i lavori della Commission on European Family Law, cfr. K.

della società attuale e, con gli opportuni adattamenti, suscettibile di essere trapiantato ⁽⁹⁸⁾ nelle diverse realtà giuridiche, sia attraverso proposte di riforma della legislazione di settore eventualmente vigente, sia come criterio interpretativo per le iniziative e gli interventi in materia o in sede giudiziaria come declinazione del principio dei cc.dd. *best interests of the child*.

La cornice entro cui effettuare i bilanciamenti e le valutazioni di politica di diritto è costituita dal seguente principio:

“Perseguire l’interesse superiore del minore di età nella dimensione digitale significa proteggere e — al pari — promuovere i diritti fondamentali degli utenti attraverso iniziative coordinate e coerenti con il sistema di responsabilità”.

Lo scenario fisiologico, abbiamo osservato, essere caratterizzato da garanzie di sicurezza rispetto ai flussi informativi, consentendo idonei livelli di disponibilità, integrità e confidenzialità dei dati concernenti gli utenti, per i quali — nella distribuzione di ruoli e responsabilità — il modello regolatorio che consideri in linea di principio le informazioni personali dei minori di età alla stregua di dati sensibili appare funzionale all’adattamento delle misure tecnico-organizzative via via più efficaci. Ciò vale per qualunque utente minore di età.

A cascata, occorre valutare le regole operazionali abilitanti i flussi di dati sensibili per individuare i fattori che possono costituire una barriera rispetto al principio espresso e quelli che, invece, si pongono in una posizione di supporto e attuazione. Ad esempio, le proposte e le iniziative regolatorie volte a proibire l’uso dei servizi e prodotti della società dell’informazione si scontrano immediatamente con l’operatività di tale principio rispetto a coloro che, seppur minorenni, abbiano acquisito capacità psicofisiche tali da poter responsabilmente realizzare la propria personalità in una dimensione globale che stimoli l’accesso a nuove esperienze e forme di conoscenza.

Occorre, pertanto, identificare le correlazioni sussistenti fra le categorie giuridiche e non relative al compimento di una certa soglia di età, la crescente capacità di discernimento, l’esigenza di garantire spazi di autonomia progressivamente più ampi, cui corrisponde una decrescente necessità di far operare la rappresentanza dell’esercente le

BOELE-WOELKI (ed), *Common Core and Better Law in European Family Law*, Intersentia, 2005.

⁽⁹⁸⁾ A. WATSON, *Legal Transplants. An Approach to Comparative Law*, Edinburgh, 1974, and Athens 1993.

responsabilità genitoriali con l'acquisizione di capacità cognitive, relazionali ed emotive sempre più vicine a quelle dell'utente adulto.

La complessità consiste nell'identificare strumenti di valutazione e monitoraggio dell'emerso carattere dinamico di ciascuna categoria.

Dall'analisi svolta in questo volume, affiorano alcune combinazioni di interventi mirati che possono coerentemente rispondere a due approcci apparentemente ispirati a interpretazioni opposte del perseguimento dell'interesse superiore del fanciullo nello spazio digitale, ma che, presentando più punti in comune, potrebbero convergere in una soluzione combinata.

I legislatori — a parità di sicurezza e livello di conformità etico-giuridica *by design* e *by default* dell'ambiente digitale e dei sistemi basati sulle tecnologie richiesti dalla normativa di settore applicabile — ben potrebbero così cogliere gli spunti più aderenti alle posizioni intraprese in materia di politica regolatoria della società dell'informazione e delle nuove tecnologie e ripensare *tout court* agli istituti giusprivatistici posti a tutela dei minori di età, in ragione delle esigenze che il tessuto sociale manifesta nel particolare contesto della dimensione digitale in questo momento storico.

9.2.1. *L'approccio anagrafico e orientato alla trasparenza.*

Nell'approccio — che vogliamo definire — “*anagrafico e orientato alla trasparenza*” sarà valorizzato l'elemento formale e certo del compimento di una determinata soglia di età. Di conseguenza, la proposta di riforma legata alla prioritizzazione dell'elemento anagrafico consiste nell'introduzione di espliciti correttivi all'istituto della incapacità di agire del soggetto che non abbia compiuto diciotto anni ritenuti ad oggi anacronistici e di fatto inapplicati ⁽⁹⁹⁾. In quest'ottica detti correttivi potrebbero trovare giustificazione nell'elencazione (non tassativa e a partire dalle interpretazioni dei diversi formanti giuridici) di attività di c.d. di ordinaria amministrazione (sia da esplicarsi nella dimensione fisica che digitale) e che potranno essere intraprese anche da soggetti minorenni, purché abbiano compiuto almeno dodici, o quattordici, o

⁽⁹⁹⁾ C. RUPERTO, *Età (dir. priv.)*, in *Enciclopedia del diritto*, vol. XVI, Milano, 1967, pp. 85 s.; P. RESCIGNO, *Capacità di agire*, in *Novissimo digesto italiano*, vol. II, Torino, 1988, p. 862; *Id.*, *Capacità di agire*, in *Digesto discipline privatistiche*, Sezione civile, vol. II, Torino, 1988, pp. 213 s.; S. PANUNZIO, *Età*, in *Enciclopedia giuridica Treccani*, vol. XIII, Roma, 1989, pp. 1 ss.

sedici anni, a seconda delle ricadute sulla sfera dei relativi diritti fondamentali. Si tratta, in altri termini, di disciplinare, sulla scia di quanto già osservato per il sistema cinese o nel dibattito dei sistemi sudamericani ⁽¹⁰⁰⁾, forme di autonomia limitata per quelle attività che non richiedano (o lo facciano solo parzialmente) interventi dell'esercente le responsabilità genitoriali in rappresentanza del minore in quanto non suscettibili di esporre la persona minorenni a rischi o pericoli, ma al contrario foriere di opportunità di crescita per lo sviluppo psicofisico ed emotivo dell'adulto di domani.

L'efficacia dell'approccio è subordinata, da un lato, al completamento di una profonda riflessione in ordine alle soglie di età cui associare spazi di capacità di agire per il soggetto minorenne; dall'altro lato, alla selezione degli spazi di autonomia, considerando le relative ricadute giuridiche nel sistema di riferimento; dall'altro lato ancora, all'individuazione di meccanismi che garantiscano parità di trattamento e di accesso alle risorse. Come corollario appare essenziale pertanto che le iniziative intraprese in questa direzione siano frutto di un processo di armonizzazione e condivisione sia delle soglie di età abilitanti spazi di autonomia del minorenne, sia delle caratteristiche delle attività che potranno essere poste in essere alla luce dei nuovi confini della (in)capacità del minorenne.

La riflessione potrebbe circoscriversi rispetto alla rilevanza giuridica del compimento di anni quattordici, da intepretarsi come minimo comune denominatore per distinguere i margini di autonomia tra bambini e adolescenti. In sistemi particolarmente sensibili a individuare un sistema a geometria variabile che possa effettivamente dar conto dell'evoluzione del minore di età durante la fase adolescenziale, tuttavia, ben potrebbero essere delineati regimi specifici per articolare ulteriormente i confini dell'incapacità del minore di anni dodici e/o per quello di anni sedici: i due scaglioni si presterebbero a innescare meccanismi di presunzione (più grave per il primo caso rispetto alla limitata autonomia del bambino, ovvero rispetto alla relativa acquisizione da parte dell'adolescente nel secondo caso) più attinenti alle esigenze rappresentate nella società attuale.

Le argomentazioni a favore dell'identificazione del compimento del quattordicesimo anno di età come soglia per distinguere i bambini dagli adolescenti si traggono da una pluralità di elementi giuridici e

⁽¹⁰⁰⁾ *Supra* Cap. 1.

fattuali. Fra tutti merita menzione l'esempio del diritto penale per il quale il compimento di tale soglia di età ha rilevanza sia in caso di soggetto attivo, escludendo l'operabilità dell'esclusione della punibilità per l'agente di una condotta illecita ⁽¹⁰¹⁾, che di vittima di un reato perpetrato da terzi, laddove si esclude il configurarsi del reato di abbandono di persona minorenni ⁽¹⁰²⁾. In particolare, se è data evidenza della capacità di intendere e di volere, da interpretarsi nella specie in relazione all'acquisizione di una certa maturità tale da comprendere il disvalore della condotta perpetrata, il quattordicenne, seppur minorenne, è perseguibile penalmente, in quanto l'ordinamento presume che a quell'età il processo di acquisizione di capacità cognitive tali da consentire di poter discernere la dimensione della liceità da quella dell'illiceità sia completato. Occorre non sottovalutare, tuttavia, il fatto che la rilevanza penale della condotta del quattordicenne si differenzia rispetto a quella dell'adulto, in quanto — a fronte del perfezionamento in entrambi dello sviluppo di capacità cognitive — mancherebbe nel primo, invero, il consolidamento di quelle abilità emotive, che scaturiscono dalla completa comprensione del sistema di valori di cui la società civile è espressione: *“pur potendo il singolo soggetto avere un livello di capacità sufficientemente sviluppato, ad esso*

⁽¹⁰¹⁾ La CRC richiede che ciascuno Stato stabilisca la c.d. MACR *“Minimum Age Criminal Responsibility”*, al di sotto della quale il minorenne non sia punibile, raccomandando di fissare la soglia al compimento del quattordicesimo anno di età, come effettivamente è previsto da 69 paesi, sebbene la media mondiale corrisponda a 11.3 anni, Committee on the Rights of the Child, *General Comment No.24 on Children's Rights in the Child Justice System*, 2019, secondo cui *“Documented evidence in the fields of child development and neuroscience indicates that maturity and the capacity for abstract reasoning is still evolving in children aged 12 to 13 years due to the fact that their frontal cortex is still developing. Therefore, they are unlikely to understand the impact of their actions or to comprehend criminal proceedings. They are also affected by their entry into adolescence. As the Committee notes in its general comment No.20 (2016) on the implementation of the rights of the child during adolescence, adolescence is a unique defining stage of human development characterized by rapid brain development, and this affects risk-taking, certain kinds of decision-making and the ability to control impulses”*.

⁽¹⁰²⁾ Il soggetto attivo è “chiunque” ai sensi dell'art. 591 c.p., l'abbandono da parte del genitore costituisce un'aggravante. Per tutti si veda il contributo di G. BASILE, *Il delitto di abbandono di persone minori o incapaci (art. 591 c.p.)*, Teoria e prassi, Milano, 2008.

mancherà quasi sempre quel bagaglio etico da cui dipende la piena comprensione dei valori morali che fondano una data comunità” ⁽¹⁰³⁾.

In altri termini, orientare le politiche di diritto al dato anagrafico non significa tralasciare la necessità di fornire spazi per accurati contemperamenti attraverso la previsione di indicazioni chiare e condivise, volte ad accertare la effettiva maturità emotiva e sociale dell'individuo rispetto alla facoltà attribuita di porre in essere una determinata condotta relazionale o contrattuale.

Per tale ragione, ai fini della nostra riflessione, appare ragionevole considerare che il quattordicenne possa — come in effetti può — compiere certe attività che siano giuridicamente rilevanti anche in autonomia rispetto ai genitori, mentre avrà bisogno del consenso/autorizzazione ovvero di essere *in toto* rappresentato dal genitore per altre attività che lo espongano nelle proprie vulnerabilità, specie quelle legate alla limitata comprensione della società.

L'importanza della valutazione della maturità emotiva e sociale diventa ancora più complessa, laddove si analizzi l'ipotesi di uniformare la soglia per l'accesso a (almeno alcuni) servizi e prodotti della società dell'informazione, che siano alla portata di minori, già al compimento degli anni dodici. In questa direzione, appare utile richiamare la *ratio* che nel nostro sistema sottostà alla fissazione dell'audizione e dell'ascolto come meccanismi obbligatori nei processi che riguardano il minorenni: tale soglia di età identifica, infatti, un momento in cui il bambino risulta in grado di esprimere il proprio punto di vista e, altresì, tutelare i propri interessi, sebbene il diritto all'ascolto, così come enunciato dalla CRC, non preveda — a tal fine — il

⁽¹⁰³⁾ Così G. DE FRANCESCO, *Diritto penale. I fondamenti*, Torino, 2011, p. 374-375 e 381 nel richiamare gli artt. 97 e 98 c.p. La giurisprudenza supera la presunzione di punibilità dimostrando che l'assenza di maturità del minore “*si fonda sulla mancanza di un adeguato « sviluppo intellettuale e morale »* (Cass. pen., sez. I, 11 luglio 1991, n. 10002) *e di una sufficiente « capacità intellettuale e di autodeterminazione »* (Cass. pen., sez. I, 1 ottobre 1990, n. 14674); *inoltre, che questa mancanza sia tale da non permettergli di rendersi conto del disvalore sociale del fatto commesso* (Cass. pen., sez. II, 13 settembre 1991, n. 9265)”, così P. BONORA, *Imputabilità del minore: educazione o rapida fuoriuscita dal processo penale?*, in *Diritto penale e uomo*, 2020, 7-8. In ottica di tutele costituzionali e capacità di discernimento, si veda il contributo monografico di C. CATERINA, *La tutela costituzionale del minore: identità, salute e relazioni*, Torino, 2023.

compimento di un'età specifica ⁽¹⁰⁴⁾. Si pensi, peraltro, che nel nostro ordinamento l'accesso a piattaforme digitali da parte del dodicenne in via autonoma per fruire di servizi scolastici è prassi consolidata anche nel nostro ordinamento ⁽¹⁰⁵⁾.

Ulteriore soglia di età che potrebbe essere oggetto di analisi ai nostri fini è quella del compimento del sedicesimo anno di età, in linea come osservato con l'art. 8 GDPR, quale età in cui il minorenne si presume capace di esprimere un consenso valido in materia di trattamento di dati per la gestione dei servizi dell'informazione ad essi destinati, come osservato nei capitoli precedenti.

In questa prospettiva, una riorganizzazione ed enunciazione di atti di ordinaria amministrazione che il minorenne — al compimento di diverse fasce di età — possa svolgere autonomamente, potrebbe porre le basi per risolvere una serie di questioni etico-giuridiche che, nella quotidianità, determinano il proliferarsi di interpretazioni inconsistenti fra loro, non dettate da una effettiva attuazione del principio dell'interesse superiore del fanciullo, quanto piuttosto da atteggiamenti opposti: eccessivamente difensivi volti a proliferare le procedure burocratiche, richiedendo in ogni caso il consenso del genitore e l'assenso all'interessato (si pensi a tal proposito alle scelte in campo sanitario, alla partecipazione del minore a sondaggi, questionari e attività di ricerca di tipo non invasivo, all'effettivo uso di strumenti digitali e tecnologie innovative); oppure — viceversa — a pratiche del tutto superficiali in quanto gli spazi di libertà e autonomia del quattordicenne risultano nell'applicazione quotidiana effettivamente sbilanciati rispetto alle richieste di conformità della regolazione delle soluzioni tecnologiche e della società dell'informazione.

Come anticipato, promuovere proposte di riforma che abbraccino siffatto approccio richiede di specificare, altresì, requisiti di forma, che consentano di distinguere, per ciascuna fascia di età, il livello di autonomia presunta dell'utente di servizi e prodotti digitali e dell'in-

⁽¹⁰⁴⁾ Gli artt. 315-*bis*, 336-*bis*, 371 c.c. e l'art. 473-*bis* c.p.c. introducono una presunzione di capacità di discernimento in ambito di contenzioso civile che riguardi il minore di età, lasciando spazio al giudice di valutare nel caso concreto se dar voce anche bambini di età inferiore. In dottrina, R. RUSSO, *La partecipazione del minore al processo nella riforma del rito civile*, in *Fam. dir.*, 2022, 647 ss.; A. ARCERI, *Il minore nel nuovo processo familiare: le regole sull'ascolto e la rappresentanza*, in *Fam. dir.*, 2022, 386 ss.

⁽¹⁰⁵⁾ DidUp, ad esempio, prevede l'utilizzo non solo da parte del genitore ma anche direttamente da parte dell'alunno mediante profilo autonomo, <https://www.argofamiglia.it>.

novazione, consentendo un intervento più restrittivo solo laddove si accerti che nella situazione concreta l'utente non abbia acquisito le conoscenze e le abilità dell'omologo — da considerarsi alla stregua dello “agente medio” — o emerga una situazione di pericolo concreto (per l'incolumità e/o la salute propria e/o di terzi, come l'uso improprio che possa far presumere lo sviluppo di dipendenze o situazioni patologiche, situazioni anche temporanee di esposizione a pregiudizi), che giustifichi il ripristino del meccanismo della rappresentanza mediante sostituzione della volontà del minore con quella dell'adulto, ovvero l'attivazione *by default* di meccanismi meno invasivi come quelli di autorizzazione e conferma da parte dell'adulto, previa notifica delle circostanze al controinteressato.

L'efficacia e l'efficienza di tale modello sono subordinate all'armonizzazione universale del *discrimen* tra il regime da applicare ai bambini e quello previsto per gli adolescenti. L'individuazione di soglie di età diverse, come osservato anche per gli spazi di autonomia ai legislatori nazionali lasciati dal GDPR, costituiscono infatti barriere alla circolazione del modello proposto, creando un effetto del tutto distorsivo e contrario al principio da cui siamo partiti, ovvero facilitare la parità di accesso alle risorse e alle opportunità della società dell'informazione in ottica di promozione dei diritti dei minori e partecipativa.

Coerentemente, dal punto di vista tecnologico, occorre che i sistemi di verifica dell'età abilitati dai prestatori di servizi digitali e dai fornitori di sistemi di intelligenza artificiale siano accurati e robusti. L'impegno, pertanto, non può essere quello a raggiungere *standard* più idonei al perseguimento della finalità — dunque come espressione di *accountability* — ma deve essere inteso come obbligazione di risultato, il cui mancato adempimento deve trovare sanzione nel sistema, incidendo — ad esempio — sull'onere della prova. Si potrebbe pensare ad una presunzione di difettosità del prodotto o di inadempimento rispetto ai termini e condizioni del servizio, salva la possibilità di identificare spazi di interpretazione più ampi per facilitare l'operare del meccanismo di prova liberatoria (non dunque limitato al caso fortuito e alla forza maggiore, ma dare la possibilità di evocare l'intervento di fattori specifici, che possano escludere la causalità). Parimenti, non sarà più sufficiente considerare l'adattamento del linguaggio delle informative agli utenti alla stregua di un mero criterio di diligenza, ma occorrerà disciplinare un vero e proprio obbligo, introducendo tra i contenuti obbligatori delle stesse altresì le conseguenze legali che il

compimento di una determinata fascia di età comporta nella sfera giuridica dell'utente.

Sia relativamente al trattamento dei dati, sia rispetto ai termini e condizioni d'uso dei servizi e dei prodotti occorrerà, perciò, introdurre specifici elementi che obblighino i titolari del trattamento, prestatori di servizi, fabbricanti, sviluppatori e *deployer* a rendere comprensibili i contenuti all'utente minorenni medio. Fattori di ordine quantitativo (ad esempio, limiti massimi oltre i quali l'informazione diventa superflua e controproducente) e qualitativo (far comprendere i meccanismi di trattamento incluse simulazioni e *tutorial* per evitare rischi o gestire e segnalare l'eventuale esposizione a pericoli, piuttosto che indicare dettagli formali) potranno fornire livelli minimi di diligenza o costruire meccanismi di accreditamento e certificazione, che consentano alle autorità competenti di verificarne la sussistenza *by default*, e il relativo aggiornamento rispetto allo stato dell'arte, nonché il mantenimento per autorizzare la messa sul mercato.

9.2.2. *L'approccio a partecipazione consapevole e personalizzata.*

Laddove si abbracci un approccio che chiameremo “*a partecipazione consapevole e personalizzata*”, orientato a valorizzare il minorenne come persona portatrice delle proprie caratteristiche a prescindere dall'età anagrafica, la proposta di ridisegnare i confini dell'incapacità del minore di età, almeno con riferimento alla dimensione digitale, si baserà sulla possibilità di attuare regimi diversi, espressione di spazi progressivi di autonomia della persona adolescente — che potranno essere accordati in ragione dell'accertamento di determinati requisiti di consapevolezza e alfabetizzazione — a prescindere dal compimento di una certa soglia di età.

Se l'utente dimostri di aver raggiunto competenze e abilità tali da far innescare meccanismi di presuzioni relativamente all'effettiva acquisizione di capacità di discernimento, cognitive ed emotive idonee a consentirgli di utilizzare in maniera fisiologica gli strumenti digitali e tecnologici, i confini dell'incapacità potranno essere riformulati nel senso di definire alcuni limiti all'operatività della rappresentanza del genitore in una serie di circostanze di uso quotidiano dei servizi e dei prodotti della società dell'informazione, a condizione che un percorso di formazione certificato, atto a sviluppare competenze e — soprattutto — consapevolezza rispetto ad un uso responsabile della dimensione digitale sia stato completato, riconosciuto, e validato in modo da

presumere che la fruizione da parte della persona minorenni possa costituire un pericolo per se stessa e/o per gli altri.

Torna anche in questo scenario la riflessione in ordine alla valutazione della capacità emotiva e sociale menzionata per corroborare l'effettività operativa dell'approccio anagrafico. A differenza di quest'ultimo, tuttavia, ivi la stessa può presumersi non tanto in ragione del compimento di una certa soglia di età, ma per il conseguimento di un bagaglio di conoscenze e abilità specifiche, che consentano di comprendere i valori che entrano in gioco nell'utilizzo di determinati sistemi.

In questo scenario, l'operatività dell'incapacità di agire tradizionalmente intesa dovrà poter essere ripristinata *by default* in caso di esposizione del minore di età a pericoli specifici, o al mutare delle circostanze soggettive (ad esempio momento di vulnerabilità psicofisica del singolo utente, oppure mancato aggiornamento del percorso formativo) od oggettive (come in caso di temporanea vulnerabilità dei sistemi, segnalazioni da parte dei prestatori di servizi digitali o del fornitore di sistemi di IA di esposizioni dell'utente a pericoli per la salute, incolumità, sicurezza o a contenuti illeciti o inidonei o inappropriati, o di uso improprio o eccessivamente prolungato, etc.), per un periodo limitato di tempo corrispondente all'effettivo bisogno del giovane.

Il ruolo della promozione della cultura dei dati e dei sistemi di IA affidabili sarebbe talmente cruciale da poter avere come effetto addirittura lo scardinamento dei presupposti dell'istituto dell'incapacità dei soggetti minori di età. L'acquisizione del bagaglio di conoscenze e abilità per poter superare i limiti imposti dal dato anagrafico e consentire all'utente singolo di realizzare la propria persona nello spazio digitale e tecnologico senza la mediazione dell'esercente le responsabilità genitoriali deve, però, poter essere valutato *a priori*, attraverso un sistema di formazione e valutazione delle competenze acquisite riconosciuto e certificato, ma anche verificato nel caso concreto dai singoli applicativi *by default*.

L'efficacia di questo approccio, infatti, è subordinata sì all'obbligatorietà di seguire un percorso formativo, non limitato all'alfabetizzazione, per poter consentire spazi autonomi di navigazione e fruizione di sistemi e di soluzioni tecnologiche. In particolare, come osservato nel corso della trattazione, si propone l'introduzione di un sistema di formazione multilivello, certificato e globale, suscettibile di aggiornamento obbligatorio e di verifica della sussistenza e mantenimento dei

requisiti di idoneità ad utilizzare responsabilmente i servizi e i prodotti della società dell'informazione. Premessa all'attribuzione di siffatti effetti giuridici all'introduzione del menzionato "patentino digitale" e — allo stesso tempo corollario — è costituita dal fatto che vi sia una armonizzata e interoperabile codificazione (o quanto meno una riconosciuta condivisione di valori etici, principi giuridici e *standard* tecnici) che consenta all'utente di poter accedere alle risorse globalmente con la stessa certificazione (*i.e.* il patentino) in quanto vi è una definizione comune di nozione di affidabilità dei sistemi, al pari di quanto avviene per la sicurezza stradale nella regolamentazione della circolazione dei veicoli e dei natanti.

In quest'ottica, si potrebbe prendere in considerazione la possibilità di individuare un sistema di *enforcement* che notifichi al genitore eventuali violazioni che possano compromettere la sicurezza, l'incolumità o la salute dell'utente e di terzi. Si pensi, ad esempio, alla possibilità che il quattordicenne, che sia autorizzato a gestire in autonomia un profilo su un *social network*, pubblichi contenuti che istighino alla violenza: a fronte della possibile decisione della piattaforma di bloccarlo e/o di limitare l'accesso all'utente, potrebbe essere previsto l'obbligo di notificare al genitore la restrizione, ovvero di costruire un sistema di monitoraggio delle attività che porti l'esercente le responsabilità genitoriali a ricevere ammonimenti rispetto alle condotte del figlio nello spazio digitale comune, oltre a innescare possibili profili di responsabilità in caso di accertamento di nesso di causalità con l'eventuale verificarsi di pregiudizi ⁽¹⁰⁶⁾.

Al pari delle sanzioni amministrative irrogate per le violazioni del codice della strada, anche la dimensione digitale potrebbe, pertanto, essere dotata di un sistema di monitoraggio, cui associare meccanismi di gestione "a punti" tali da portare in caso di decurtazione anche alla sospensione del patentino digitale, con l'obbligo per il minorenni di sostenere nuovamente i corsi di formazione e gli esami di valutazione per poter di nuovo fruire, in autonomia, dei servizi e dei prodotti della società dell'informazione.

Il sistema ben potrebbe essere dapprima istituito a tutela degli utenti minori di età per poi estendersi a tutti gli utenti.

⁽¹⁰⁶⁾ Da cui la possibile attuazione di regimi di assicurazione obbligatoria, discussi *supra*.

9.2.3. *La combinazione dei due approcci.*

La combinazione dei due approcci presentati è quello che, valorizzando la persona umana *per se*, possa in primo luogo assicurare certezza del diritto e innescare meccanismi di tutela a partire da dati certi, come l'età, per poi consentire una personalizzazione orientata a valorizzare la partecipazione diretta nelle attività e nei processi decisionali, che siano alla portata dello sviluppo psicofisico dell'utente, sia cognitivo che emotivo, del relativo bagaglio di competenze e abilità necessarie per fruire delle opportunità della società dell'informazione e, allo stesso tempo, prevenire (o gestire) l'esposizione a eventuali rischi.

Si propone pertanto di combinare alcuni elementi dell'approccio anagrafico con quello a partecipazione consapevole e personalizzata al fine di costruire un sistema dinamico non solo di accesso alle risorse, ma anche di monitoraggio dell'uso, al fine di consentire efficaci interventi nel caso in cui dalla dimensione fisiologica dei rapporti personali e contrattuali si passi, per qualsivoglia ragione, ad una situazione (anche momentanea) di patologia.

In una società di dati in cui si valorizzano le caratteristiche di personalizzazione, predizione, prevenzione e partecipazione (le cc.dd. 5P ad esempio della Medicina Personalizzata, Predittiva, Preventiva, Partecipatoria, e basata sulla Popolazione) ⁽¹⁰⁷⁾, il modello che maggiormente si presta ad essere trapiantato in una pluralità di sistemi è quello che vede l'introduzione di correttivi all'incapacità del minorenni al verificarsi di una duplice condizione: da un lato, il compimento di una certa soglia di età — che nel presente contributo si suggerisce poter essere identificata con il quattordicesimo anno — e, dall'altro, l'acquisizione di un bagaglio culturale e di abilità rispetto alla dimensione digitale che renda il singolo utente consapevolmente partecipe e responsabile delle proprie azioni e degli spazi di autonomia progressivamente sempre più ampi acquisibili, attraverso un percorso di formazione e alfabetizzazione che risponda a regole trasparenti, certificate e riconosciute.

Per tale ragione il percorso che porti all'ottenimento del mezzionato "patentino digitale" potrebbe essere suddiviso in tre livelli: i primi due

⁽¹⁰⁷⁾ J. BORRÁS-BLASCO, E. RAMÍREZ-HERRÁIZ, A. NAVARRO-RUIZ, *Integration of persistence in the 5P-medicine approach for age-related chronic diseases*, Int J Qual Health Care, 2024 Apr 22;36(2):mzae026. doi: 10.1093/intqhc/mzae026. PMID: 38581657.

in ottica di sensibilizzazione illustrando i rischi, le opportunità e le modalità di funzionamento di piattaforme digitali di uso comune e sistemi basati sull'IA a portata di minori di età, questi due moduli potrebbero accompagnare i programmi curriculari delle attività di educazione civica e tecnologia della quinta elementare e della prima media, attraverso una verifica delle competenze acquisite al termine di ciascun modulo. Un terzo livello, da svolgersi nel successivo biennio, potrebbe consentire allo studente di applicare le conoscenze acquisite e simulare possibili situazioni, con l'obiettivo di associare a nozioni teoriche anche lo sviluppo di abilità di prevenzione dei rischi e risoluzione dei problemi. In quest'ottica, al compimento del quattordicesimo anno di età, lo studente potrebbe sostenere l'esame completo per l'ottenimento della certificazione che gli consentirà, oltre che di esprimere un consenso valido per il trattamento dei propri dati strumentale all'utilizzo di servizi della società dell'informazione — ai sensi dell'8 GDPR o nel nostro ordinamento dell'art. 2 *quinqüies* del Codice della Privacy — di poter accedere alle applicazioni, che siano “*a misura di adolescente*” attraverso sistemi di controllo parentale meno stringenti rispetto a quelli necessari per i bambini e per coloro che non abbiano invece ottenuto il patentino, visto dunque come meccanismo di certificazione del livello minimo di alfabetizzazione.

La proposta appare suscettibile — con gli opportuni adattamenti — non solo di circolare nei diversi sistemi giuridici, ma anche di essere applicata ad utenti non necessariamente incapaci, potendo realizzare — attraverso la valorizzazione della cultura dei dati delle tecnologie — ambienti e sistemi digitali più sicuri e alla portata delle persone tutte ⁽¹⁰⁸⁾, in quanto portatrici ciascuna delle proprie vulnerabilità e dei proprie potenzialità, mutuando dall'esempio delle misure tecniche e organizzative introdotte nel settore della circolazione stradale.

⁽¹⁰⁸⁾ O. BEN-SHAHAR - A. PORAT, *Personalized Law: Different Rules for Different People*, cit.

**LA MITIGAZIONE DELLE VULNERABILITÀ NELLA
SOCIETÀ DELL'INFORMAZIONE: COSTRUIRE
COMPETENZE E PROMUOVERE TUTELE
A GEOMETRIA VARIABILE**

SOMMARIO: 1. L'approccio basato sulla valutazione del rischio e il sistema di tutele a geometria variabile volto alla costruzione di competenze. — 2. Decostruire l'incapacità: mitigare le vulnerabilità del minore, costruendo competenze e abilità. — 3. Non ho l'età, ma... ho il patentino: circolazione del modello e implicazioni sui paradigmi di responsabilità... — 4. (*Segue*). ... interessi superiori, (in)capacità e dignità del minore di età.

1. L'approccio basato sulla valutazione del rischio e il sistema di tutele a geometria variabile volto alla costruzione di competenze.

La datificazione della società ha portato ad un radicale cambiamento nei mezzi di comunicazione e nelle metodologie di osservazione ed analisi della realtà, spostando il baricentro verso una nuova dimensione, quella caratterizzata dall'accessibilità e fruibilità di servizi e prodotti digitali in misura potenzialmente indiscriminata, rispetto ai paradigmi legati alle logiche possessorie e proprietarie proprie della dimensione fisica. Come abbiamo visto, lo spazio digitale è governato da dinamiche che si dipanano attraverso modalità comuni e prescindono dalle caratteristiche personali degli utenti o dal luogo di accesso ai servizi.

Nonostante l'assenza di barriere geografiche, la relativa regolamentazione è demandata a competenze legislative nazionali o, come nella strategia della Commissione UE, sovranazionali, o — eventualmente — attraverso Convenzioni internazionali in cui sono formulate norme di principio, le quali non rispondono, tuttavia, alle specifiche esigenze emergenti nei diversi settori economici. I tratti comuni alle iniziative legislative, anche di settore, pur percependo i bisogni derivanti dal profondo mutamento dei processi organizzativi — determinato dalla

transizione digitale di servizi e prodotti — non raggiungono livelli di armonizzazione e omogeneità soddisfacenti.

Eppure tutti gli utenti nella loro diversità esprimono — al contempo — fragilità e potenzialità di realizzazione della propria persona analoghe nella dimensione digitale. Gli operatori economici si trovano inoltre di fronte alle stesse sfide: proteggere le infrastrutture che consentono la fruizione dei servizi (al pari dei locali e dei luoghi fisici), promuovere la dignità della persona e gli altri diritti fondamentali degli utenti-consumatori nelle relazioni contrattuali, trarre profitto (laddove pertinente).

L'affresco delle iniziative legislative che interessano la società dell'informazione e le nuove tecnologie che abbiamo tracciato nei capitoli precedenti ha evidenziato una serie di indici rilevanti.

In primo luogo, l'assenza di una correlazione tra il livello di avanzamento tecnologico del sistema giuridico dal punto di vista economico e l'attenzione della relativa legislazione verso la persona-utente. In particolare, a partire dalla protezione dei dati, abbiamo colto l'interesse a fornire una tutela appropriata ai soggetti deboli prevenendo possibili esposizioni a discriminazioni e abusi dovuti ad un uso improprio delle informazioni personali trattate, il cui conferimento, tuttavia, risulti necessario per l'utilizzo dei servizi e dei prodotti digitali stessi.

Ed è proprio in contesti lontani dall'Unione Europea — e non necessariamente tecnologicamente avanzati — che abbiamo potuto apprezzare, in secondo luogo, possibili risposte efficaci elaborate soprattutto per proteggere categorie di soggetti considerati vulnerabili. Ad esempio, abbiamo considerato positivamente l'equiparazione indiana o dello Swaziland di tutte le informazioni concernenti utenti minori di età al regime speciale previsto nei rispettivi sistemi per i dati cc.dd. sensibili.

Dal punto di vista della tecnica legislativa, abbiamo potuto osservare come la protezione del soggetto interessato considerato vulnerabile (nella specie, il paziente e il minore di età) porti a connotare la natura dell'informazione personale trattata e di conseguenza applicare condizioni di liceità specifiche (*rectius* limitate) e al contempo richiedere una analisi più profonda ai titolari del trattamento nell'eseguire la valutazione dei rischi e nell'implementare misure tecnico-organizzative capaci di proteggere i flussi di dati nelle circostanze concrete. Oppure, in maniera ancora più accurata, come specifica la formulazione discussa in Brasile, sono solo i dati dei bambini (e non anche quelli degli

adolescenti) a poter essere trattati secondo basi giuridiche ancora più ridotte (come il consenso del legale rappresentante o in caso di emergenza), rendendo operativa anche nell'ambito digitale un sistema di tutela differenziato per fasce di età, proprio di quel sistema giusfamiliaristico.

Diversamente, abbiamo commentato criticamente altre soluzioni, come quelle approvate in Australia o proposte da alcuni legislatori statunitensi, tese a introdurre divieti basati sul semplice dato formale del compimento di una determinata età anagrafica per l'uso di servizi e prodotti della società dell'informazione, in quanto non aderenti all'attuale evoluzione dei rapporti tra consociati: ad oggi sarebbe infatti difficilmente imponibile un divieto di uso di piattaforme *social network* o di prodotti basati su IA ai minorenni, sia in quanto ampiamente diffusi nella quotidianità di adolescenti, sia per la complessità di introdurre misure adeguate di *enforcement* senza intaccare le libertà fondamentali delle persone.

Nel corso della trattazione abbiamo invero privilegiato la prospettiva di costruzione di competenze e abilità volte a promuovere una cultura responsabile dei dati e delle tecnologie al fine di superare la tensione tra rischi e opportunità derivanti dalla datificazione della società.

A corroborazione, abbiamo declinato i principi di responsabilizzazione e alfabetizzazione (ancora più efficaci nella formulazione in lingua inglese nei termini di *accountability* e *literacy*) che guidano gli operatori economici nei rapporti tra privati e rispetto ai diritti fondamentali dei bambini e degli adolescenti ad essere istruiti ed educati rispetto alle attuali sfide che la società propone alle generazioni cc.dd. native digitali.

Abbiamo osservato come la necessità di avviare un processo culturale di responsabilizzazione verso l'uso delle tecnologie sia largamente condivisa: le organizzazioni internazionali (dall'UNICEF, al CoE), la Commissione Europea stessa, le istituzioni (governi nazionali, autorità garanti, enti locali, etc.) ad ogni livello promuovono strategie ed interventi per elevare il livello di consapevolezza degli utenti nella dimensione digitale. Sensibilizzare l'utente diventa una misura complementare rispetto all'imposizione di obblighi di protezione *by design* e *by default* imposti agli operatori economici.

Abbiamo osservato, infatti, come l'approccio basato sulla valutazione, mitigazione e monitoraggio dei rischi promosso dall'UE — e trapiantato in molti altri sistemi — richieda una riflessione tutt'altro

che superficiale relativamente sia alle vulnerabilità comuni alle diverse categorie di utenti, sia a quelle specifiche del singolo individuo in relazione alla particolare applicazione o soluzione tecnologica. Anche attraverso interventi delle autorità garanti per la protezione dei dati (come per il caso *Open AI* o il più recente *Deep Seek*), abbiamo individuato la stretta correlazione tra datificazione dei servizi e dei prodotti e nuove tecnologie, che si articola nel rispetto dei principi informatori della materia, tra cui — oltre all'*accountability* — quello di trasparenza che ha giocato un ruolo particolarmente rilevante nell'affermare una prospettiva umano-centrica nell'introduzione di strumenti innovativi accessibili alla cittadinanza anche (e soprattutto) a titolo gratuito. Anche i grandi colossi tecnologici, infatti, devono giustificare le proprie scelte tecniche e organizzative volte a mitigare i rischi e i pericoli per i soggetti interessati o destinatari dei servizi, specie se utenti vulnerabili, e porre ciascuna persona interessata nelle condizioni di conoscere, capire, ed essere in grado di mantenere il controllo sulle proprie informazioni ed esercitare i relativi diritti, ciò anche prima che il DSA entrasse in vigore. Si tratta di attuare i valori della Carta dei Diritti Fondamentali dell'Unione Europea più che dar seguito a specifici obblighi richiesti da una singola normativa di settore.

In questa prospettiva, l'adozione dell'approccio basato sulla valutazione del rischio costituisce la formula legislativa volta ad instaurare una relazione di affidamento tra chi detiene il controllo (*rectius* il governo) dell'informazione fornita dal soggetto interessato e quest'ultimo; tra chi tratta le informazioni anche con strumenti automatizzati e sistemi di IA e il destinatario del meccanismo ovvero del risultato dell'applicazione, a prescindere dalla sussistenza di un vincolo contrattuale diretto. Infatti, gli obblighi di valutazione e mitigazione dei rischi insistono su chi detiene il controllo del dato anche laddove la base giuridica del trattamento dei dati non presupponga la sussistenza di un contratto diretto con il soggetto interessato.

A questo proposito, i principi di affidabilità (utilizzato per dichiarare la conformità etico-giuridica dei sistemi di intelligenza artificiale) e di *accountability* (volto ad introdurre il piano della responsabilizzazione in ottica preventiva sulla scia del principio di precauzione nella strategia europea dei dati) utilizzati dal legislatore comunitario stanno in equilibrio come due piatti della stessa bilancia, affinché i valori dell'UE siano considerati rispettati e attuati *by design* e *by default* in ogni scenario applicativo. Gli stessi, peraltro, assumono una portata più vasta, transfrontaliera, legata all'esigenza comune alle legislazioni che

abbiamo analizzato di poter inequivocabilmente identificare ruoli e responsabilità in capo a soggetti capienti, capaci cioè di rispondere (*i.e.* riparare o risarcire) in caso di evoluzione patologica del rapporto tra consociati nell'utilizzo di prodotti o servizi digitali. Spetta dunque all'operatore economico a seconda del ruolo (*i.e.* nel diritto dell'UE, specificamente al titolare del trattamento, al prestatore di servizi digitali, allo sviluppatore, al fornitore o al *deployer* di sistemi di IA) garantire il rispetto e la protezione della persona e dei gruppi di persone, specie se vulnerabili, dal possibile abuso o uso improprio degli strumenti tecnologici che vada a compromettere l'esercizio se non addirittura violare i diritti fondamentali della persona, cagionando un danno risarcibile ⁽¹⁾.

Nella sconfinata dimensione digitale emerge, dunque, una tendenza nuova rispetto alla regolamentazione dei rapporti fra consociati nella dimensione fisica: quella legata alla tecnica legislativa che sempre più spesso apre alla predisposizione di strumenti di tutela a geometria variabile. Accettando che l'attuazione delle tutele sia demandata alla percezione dei rischi e alla relativa mitigazione nell'ambito delle procedure di valutazione d'impatto (*rectius* degli impatti) sui diritti fondamentali della persona, infatti, affiora una sorta di diritto ritagliato alle esigenze dello specifico scenario, suscettibile di mutare in ragione di fattori oggettivi e soggettivi.

In questa prospettiva, prende forma una sorta di personalizzazione del diritto ⁽²⁾, intesa sia come tendenza a valorizzare la componente umano-centrica nelle scelte legislative e interpretative, sia come valorizzazione della singola esperienza non solo delle istanze di tutela, ma anche delle relative risposte da fornire in ottica preventiva, onde evitare che il rischio identificato si manifesti e, anche laddove ciò accada, per garantire che le relative conseguenze possano essere mitigate, se non addirittura annullate nelle circostanze concrete.

I menzionati fattori oggettivi o soggettivi che caratterizzano il

⁽¹⁾ Giova ricordare la giurisprudenza della Corte di Giustizia dell'UE che ha in più occasioni ribadito che ai fini della risarcibilità del danno derivante dalla violazione della normativa sulla protezione dei dati personali debba essere provato il nesso di causalità tra la violazione e le conseguenze pregiudizievoli che non sono automaticamente risarcibili, negando purtuttavia la sussistenza di soglie di gravità emergenti dal testo del GDPR, E. C.J., c. 300-21, Österreichische Post, 3.5.2023.

⁽²⁾ O. BEN-SHAHAR - A. PORAT, *Personalized Law. Different Rules for Different People*, cit.

singolo scenario, da un lato, sono generati dall'interpretazione delle circostanze di fatto a partire dalle categorie giuridiche tradizionali applicabili al caso concreto, richiedendo all'operatore di specificare le misure di salvaguardia necessarie per attuare le forme di protezione desiderate nella dimensione digitale, e, dall'altro, danno luogo a loro volta a implicazioni di sistema che si pongono in tensione con le correnti interpretazioni degli istituti di diritto privato posti a tutela dei paradigmi su cui si fondano i rapporti tra consociati nella dimensione reale. Quest'ultimo profilo al contempo, tuttavia, testimonia i passaggi evolutivi delle relazioni fra privati e fra privati e imprese nelle more della transizione digitale di servizi e prodotti che comunemente sono riferibili al fenomeno della "datificazione" della società ⁽³⁾.

Abbiamo osservato come il paradigma della proprietà e del possesso siano oggi superati nella dimensione digitale dalle peculiarità del governo dei dati: accesso, condivisione, riuso delle informazioni per le finalità più svariate costituiscono i motori del mercato digitale.

A fronte della frammentarietà della gestione delle attività di conformità alle diverse iniziative che insistono sulla società dell'informazione e dell'innovazione tecnologica, abbiamo notato che ciò che dovrebbe tenere il sistema in equilibrio e consentire una applicazione omogenea e paritaria in realtà subisce ulteriori effetti distorsivi. L'apparato sanzionatorio, infatti, è costituito dai meccanismi di *enforcement* e dalle attività di monitoraggio e controllo da parte delle autorità indipendenti competenti per materia che operano, *ratione materiae*, ma cooperando in *task force* affinché i principi comuni possano trovare diretta applicazione in caso di manifesta violazione dei diritti fondamentali della persona.

Il mercato, invero, in una società consapevole e responsabile dovrebbe poter essere influenzato in larga misura dall'affidabilità riposta dagli utenti. Infatti, essendo alimentato dagli stessi soggetti interessati, che sono il perno attorno al quale ruotano le istanze di protezione, ci si dovrebbe aspettare che le eventuali falle nella protezione degli utenti stessi possano avere ricadute drastiche sull'utilizzo del dato servizio o prodotto. Orbene, abbiamo osservato come la limitazione temporanea del trattamento imposta ai prestatori di servizi digitali gratuiti (si pensi ai fornitori di servizi basati su intelligenza artificiale di

⁽³⁾ G. MASCHERONI - A. SIIBAK, *Datafied Childhoods. Data Practices and Imaginaries in Children's Lives*, P. Lang., 2022.

tipo generativo, come il caso OpenAI o Deep Seek) o le relative condanne a sanzioni pecuniarie (si pensi ai *social network*) non abbiano tuttavia dissuaso gli utenti né alla sottoscrizione di profili, né all'utilizzo delle relative funzionalità. Ciò vale tanto per gli utenti adulti che per quelli più vulnerabili ⁽⁴⁾.

In quest'ottica, i meccanismi di protezione non possono più prescindere dal confrontarsi con la componente socio-culturale: affinché il sistema di tutele improntato sulla valutazione dei rischi sia efficace, occorre che l'agente medio abbia un bagaglio di conoscenze e competenze (anche tecniche) capaci di far fronte ai pericoli di ordinaria amministrazione.

L'educazione digitale per acquisire le nuove conoscenze e competenze che la datificazione della società richiede per poter sfruttare le opportunità di realizzazione che l'innovazione tecnologica ci offre in ogni settore economico diventa una priorità tanto per gli operatori, quanto per i singoli cittadini di ogni età, di ogni luogo, di ogni condizione socio-economica, etc.

2. Decostruire l'incapacità: mitigare le vulnerabilità del minore, costruendo competenze e abilità.

Approfondendo le molteplici iniziative relative alla tutela e promozione dei diritti dei minori di età in sistemi appartenenti a tradizioni giuridiche diverse, abbiamo osservato come bisogni e relative risposte tecnico-organizzative per proteggere i minori di età attraverso la rappresentanza legale del genitore possano richiedere degli adattamenti nella dimensione digitale volti a promuovere una prospettiva più partecipativa.

Abbiamo discusso come la limitata capacità di discernimento dei bambini, che si pone alla base delle scelte normative volte ad escludere la capacità di agire, appare dotata invero di nuove sfaccettature che potenzialmente possono, di pari passo con lo sviluppo cognitivo, sviluppare competenze e abilità per formare pensiero critico sufficientemente maturo per poter consentire di accompagnare la propria

⁽⁴⁾ OECD (2014), *OECD Regulatory Compliance Cost Assessment Guidance*, OECD Publishing. <http://dx.doi.org/10.1787/9789264209657-en> e più di recente A. CUEVAS, *Assessing the Economic Effects of GDPR Compliance on European Businesses*, Vol. 7 No. 2 (2024): *Economic Review of the European Union*, 1 ss.

crescita anche attraverso servizi e prodotti della società dell'informazione in maniera sempre più autonoma e meno supervisionata dal genitore, anziché rimanere formalmente esclusi, ovvero essere rappresentati (spesso fittiziamente) dagli adulti, senza consentire peraltro l'attivazione di tutele *ad hoc* in caso di uso inappropriato.

Abbiamo osservato, infatti, come gli istituti codicistici che derivano dall'incapacità del minore siano stati originariamente volti a proteggere il patrimonio e la certezza degli scambi ⁽⁵⁾, profili del tutto estranei rispetto alle vulnerabilità digitali derivanti dai rischi propri della società dell'informazione e delle nuove tecnologie. Peraltro, il meccanismo di tutela in materia contrattuale si fonda sull'eccezionalità per l'interessato minorenni di trovarsi a porre in essere atti giuridici rilevanti: si pensi all'istituto dell'emancipazione per consentire al minore di età di contrarre matrimonio o alle condizioni che abilitino l'ingresso al mondo del lavoro per il sedicenne ⁽⁶⁾. Nell'ambiente digitale, invero, l'accesso ai servizi e prodotti è non solo divenuto quotidiano, come mezzo di comunicazione, ma altresì indispensabile per poter crescere e formare la propria personalità: abbiamo richiamato nei precedenti capitoli la rapida evoluzione delle tecnologie per l'educazione e l'istruzione, ad ogni livello e grado, come opportunità di costruire un bagaglio culturale che includa nuove abilità tecnico-informatiche che sono (già) necessarie per affrontare le sfide attuali e future.

La rivoluzione tecnologica ha un effetto talmente pervasivo da non poter escludere i giovani da una contaminazione che porti a sviluppare conoscenze, competenze e abilità per partecipare direttamente e attivamente al cambiamento socio-culturale che stiamo attraversando e poter beneficiare delle opportunità di realizzazione dei propri interessi al pari degli adulti, in quanto persone e cittadini (e non solo soggetti minori, ovvero incapaci) ⁽⁷⁾.

Il perseguimento dell'interesse superiore del fanciullo, pertanto,

⁽⁵⁾ Sul dibattito in ordine alla necessità di attualizzare gli istituti codicistici ad una interpretazione costituzionalmente orientata degli stessi, si vedano i contributi nel corso del tempo di R. NICOLÒ, voce *Diritto civile*, in *Enc. dir.*, XII, Milano, 1964, 904 ss.; P. RESCIGNO, *Per una rilettura del codice civile*, in *Giur. it.*, 1968, IV, c. 20; Id., *I manuali di diritto privato dopo la Costituzione*, in *Riv. dir. civ.*, 1998, I, 409 ss.; P. GROSSI, *Scienza giuridica italiana. Un profilo storico 1860-1950-2000*, Milano, 2000; N. LIPARI, *Il diritto civile tra legge e giudizio*, Milano, 2017.

⁽⁶⁾ Art. 3 c.c. e Direttiva 94/33/CE del Consiglio, del 22 giugno 1994, relativa alla protezione dei giovani sul lavoro.

⁽⁷⁾ Per tutti: F.D. BUSNELLI, *Capacità ed incapacità di agire del minore*, cit.

non può essere interpretato come barriera protettiva escludente, ma deve essere letto in ottica costruttiva, considerando le condizioni e le circostanze del caso concreto. Aumentano e si diversificano, dunque, le istanze di tutela, non più legate esclusivamente alla protezione del patrimonio dell'incapace (e dei rappresentanti legali che rispondono per loro) e della certezza degli scambi tra contraenti, ma rivolte alla protezione di ulteriori beni: l'incolumità fisica e psichica, la vita privata, i dati personali e la confidenzialità, la libertà di esprimere la propria opinione e di associarsi, il diritto al gioco e alla creatività, etc. Questi ultimi richiedono l'innescarsi di forme di protezione del tutto diversificate rispetto a quelle tradizionali: consentire al minorenne di cogliere le opportunità che la digitalizzazione offre per crescere e realizzare la propria persona nella società attuale non è una facoltà che istituzioni, famiglie e comunità di riferimento possono (o meno) concedere al nativo digitale, ma un vero obbligo giuridico che deriva dal principio del perseguimento dell'interesse superiore dei fanciulli in ogni atto e iniziativa che li concerne.

L'adozione di meccanismi basati sulla valutazione del rischio che allocano ruoli e responsabilità in maniera granulare agli operatori economici, alle istituzioni e a chi esercita responsabilità genitoriali o educative verso il singolo bambino consente di raccogliere i presupposti per far circolare buone prassi da eventualmente replicare con adattamenti in contesti simili tra loro, dando vita a processi virtuosi di adeguamento ad un quadro normativo, piuttosto che ad un altro, con il comune intento di tutelare i bambini dai pericoli che il trattamento di informazioni personali, contenuti accessibili, o strumenti di profilazione possono arrecare per la relativa incolumità fisica, psichica e sicurezza personale.

Questo minimo comune denominatore è stato utilizzato non solo per un'opera di sistematizzazione delle normative vigenti alla luce dei comuni rischi e delle misure di mitigazione per l'utente medio minorenne, ma anche — da un lato — per trarne indicazioni di *policy* per la costruzione di un ecosistema digitale a portata di bambino e dell'adolescente e — dall'altro lato — per compiere una riflessione più generale in materia di vulnerabilità.

In particolare, abbiamo osservato come — in contesti socio-economici ben diversi dall'Unione Europea — la protezione e la promozione dei diritti dei minori di età nella dimensione digitale siano attenzionate con strumenti giuridici suscettibili di trovare non solo

idonea implementazione, ma anche di impattare notevolmente sulle categorie giuridiche analizzate nel corso della trattazione.

Il caso di studio dei minori di età nella dimensione digitale, infatti, ha consentito di riferirsi a un utente, che può essere esposto ad alcuni rischi e pericoli specificamente indirizzati all'immaturità psicofisica, cognitiva ed emotiva a comprendere cosa sia finzione (e cosa sia realtà) e le relative implicazioni nel breve e lungo termine, ma ha anche permesso di guardare al concetto di vulnerabilità, come una condizione — multiforme rispetto alle modalità di esposizione ai rischi, durata, e gravità — comune a tutti gli utenti di servizi e prodotti della digitalizzazione.

Il bambino, infatti, proprio per la duttilità del pensiero in formazione acquisisce progressivamente abilità e capacità per poter innalzare il livello di supervisione e controllo delle proprie azioni, raggiungendo progressivamente l'età formale e gli strumenti cognitivi per essere equiparato all'utente medio adulto, cui si applica il canone della diligenza del buon padre di famiglia. Il modello dell'utente medio adulto, tuttavia, non può essere concepito come un punto di arrivo perché raggiungere la maggiore età non esime dall'esposizione ai medesimi rischi, cui si aggiungono, da una parte, una responsabilità patrimoniale e, dall'altra, il venir meno delle misure di protezione introdotte *by default* per i bambini, che non è detto siano sostituibili dalla ragionevolezza dell'adulto ⁽⁸⁾.

Da questo punto di vista, abbiamo concepito la vulnerabilità del minore di età da valutare nel caso concreto, secondo il principio dei vasi comunicanti, laddove contestualmente si manifestino altri profili ostativi all'inclusivo uso di un prodotto o servizio (si pensi all'utente appartenente ad una minoranza linguistica o etnica in un determinato scenario, ovvero in quanto paziente o disabile in un altro ancora, etc.), apprezzandone altresì la possibilità che certe circostanze — anche temporanee — possano essere rappresentative di una serie di implicazioni che non siano foriere di esposizione a rischi specifici per il proprio

⁽⁸⁾ Si pensi alle quotidiane esposizioni a violazioni rispetto alla sfera privata e confidenziale, dovuta all'imprevedibilità di possibili blocchi o attacchi alle infrastrutture e ai sistemi informatici, ovvero ai rischi di stigmatizzazione sociale (anche non diretta) dovuta all'estrazione e aggregazione delle grandi moli di dati, alla manipolazione del pensiero attraverso misinformazione, con ricadute sui processi economici, industriali, democratici, nonché alle implicazioni che l'introduzione di nuove tecnologie negli assetti organizzativi non ancora esplorati.

benessere o, viceversa, esserlo per una pluralità di motivi di discriminazione.

Se il concetto di vulnerabilità multiple è caratterizzato dalla dinamicità, in quanto suscettibile di mutamenti nel tempo e, persino dalla reversibilità, in quanto l'acquisizione di competenze specifiche può senz'altro consentire di sviluppare e interiorizzare abilità di prevenzione e gestione dei possibili pericoli. Allo stesso modo, andrebbe concepita la posizione reciproca di "non-vulnerabilità". Infatti, rispetto alle nuove tecnologie e alla datificazione della società nessuna persona può considerarsi immune rispetto al pericolo di compromissione dei propri diritti fondamentali, al pari della esposizione a catastrofi ed eventi naturali. La differenza con questi ultimi risiede nella probabilità non remota che un rischio si verifichi in ragione della continua esposizione alla circolazione dei flussi informativi e dell'uso delle tecnologie nella vita quotidiana.

Di conseguenza, la capacità legale di agire necessita di una rivisitazione e di un adattamento quanto meno rispetto alle caratteristiche dei servizi e prodotti propri della dimensione digitale. Da un lato, infatti, il compimento della maggiore età, ovvero di un'età diversa da quella di anni diciotto, non può costituire (l'unico) elemento per abilitare un uso consapevole e responsabile dei prodotti e dei servizi della società dell'informazione. Dall'altro lato, l'età anagrafica e la relativa verifica possono rappresentare una robusta presunzione di "non-vulnerabilità" solo laddove tutti gli utenti maggiorenni possano dare evidenza di aver acquisito capacità e abilità tecniche (ovvero un livello alfabetizzazione rispetto ai sistemi basati sull'IA) ritenute sufficienti per tracciare le caratteristiche dell'utente medio. Il che significa poter ragionevolmente considerare acquisita nel bagaglio culturale una serie di conoscenze e competenze sulla datificazione della società che rendono il singolo capace di percepire (e dunque prevenire) i pericoli e i rischi, comprendere i confini della sfera di liceità e illiceità ed assumersi le conseguenti responsabilità, apprendendo abilità di adottare contromisure per annullare o minimizzare conseguenze negative di utilizzi impropri.

In questa prospettiva, dunque, percorsi di sensibilizzazione, formazione e alfabetizzazione richiedono un processo di standardizzazione e certificazione capace di irrobustire la presunzione di "non-vulnerabilità" per l'utente che soddisfi il requisito formale (*rectius* anagrafico), ma anche capace di accertare l'acquisizione di una graduale autonomia di coloro che si avvicinino a maturità psico-cognitiva,

corrispondente, come abbiamo visto, generalmente a certe soglie di età (*i.e.* in sintesi 12 anni per l'ascolto obbligatorio, 14 anni per la punibilità, dai 13 ai 16 anni per esprimere consenso valido sul trattamento dei dati personali) per essere considerati capaci di agire nei limiti previsti dal sistema di tutele giusprivatistiche.

La costruzione di competenze e abilità a partire dai giovani utenti non può rimanere un mero esercizio di *accountability* o di adempimento agli obblighi di alfabetizzazione per gli operatori economici della società dell'informazione o delle istituzioni. Occorre integrare l'offerta educativa nell'ambito dell'istruzione obbligatoria con percorsi di formazione e sensibilizzazione all'uso dei servizi e prodotti digitali e allo sviluppo di competenze tecniche come elementi base del bagaglio culturale del bambino per affrontare le sfide quotidiane.

Il passo ulteriore, proposto nel presente contributo, è quello di consentire di valutare l'acquisizione di determinate competenze per autorizzare forme di autonomia dell'adolescente come utilizzatore della dimensione digitale. Il paragone con la circolazione stradale è apparso quanto mai appropriato per definire i confini della proposta.

È dato di fatto che la società dell'informazione e le nuove tecnologie siano accessibili ai minori di età. È altresì constatato che il controllo parentale (ovvero di coloro che esercitano la rappresentanza legale o gli educatori) sia lasciato alla gestione del *ménage* quotidiano e possa essere facilmente eluso vuoi per i tempi e i modi di utilizzo delle nuove tecnologie che spesso non consentono di prevenire i rischi e i pericoli. È altresì certo che le misure tecnico-organizzative di protezione imposte agli operatori economici non sono da sole sufficienti ad evitare l'esposizione degli utenti ai rischi propri della dimensione digitale.

D'altro canto, le tecnologie sono sufficientemente mature per poter effettuare delle verifiche rispetto a certi parametri, come l'età dichiarata dall'utente, ma anche — laddove previsti — il possesso di eventuali requisiti abilitanti e limitare le funzionalità del servizio o del prodotto alla verifica di una pluralità di condizioni.

La proposta formulata nei precedenti capitoli è pertanto quella di sviluppare un percorso di formazione certificato e accreditato capace di accertare l'acquisizione di conoscenze teoriche e competenze pratiche per abilitare l'adolescente ad utilizzare in maniera autonoma servizi digitali e i prodotti tecnologici che siano ragionevolmente destinati agli stessi. Si tratterebbe di conferire, al pari della licenza di guida, un titolo

abilitante per poter “navigare in acque”, che siano sicure *by design e by default*, in quanto suscettibili di essere percorse da utenti minorenni.

Nel capitolo precedente abbiamo ipotizzato anche possibili modalità di gestione del possesso del proposto patentino digitale da parte degli operatori economici: potrebbe essere richiesto come condizione necessaria in sede di apertura di un profilo sulle piattaforme di grandi dimensioni ai sensi dell’art. 33 del DSA oppure per l’utilizzo di certi sistemi basati sull’IA. Per cui, in presenza di patentino potrebbe essere richiesto il dato di contatto del legale rappresentante per consentire la trasmissione di messaggi di allerta in caso di violazioni dei termini e condizioni d’uso da parte dell’utente minorenne, di autorizzazione all’abilitazione di specifiche funzionalità che esponcano maggiormente ai rischi (ad es. abilitazione ad effettuare transazioni entro certi limiti, possibilità che il profilo possa essere oggetto di contatto da adulti, etc.), lasciando per la navigazione ordinaria l’adolescente consapevole di utilizzare il sistema.

In altri termini, nella fisiologia dell’utilizzo dei servizi e prodotti digitali, l’adolescente munito di patentino potrà ritenersi ragionevolmente autonomo, mentre, laddove vi sia una situazione che viri alla patologia o nella criticità si dovranno poter innescare quei meccanismi di allerta e prevenzione di eventuali danni, coinvolgendo sussidiariamente il legale rappresentante.

La proposta pare sostenibile e attuabile: uno schema di formazione e certificazione per gli adolescenti risponde, infatti, a una pluralità di esigenze condivise nei diversi sistemi giuridici e al contempo ben si presta a ottemperare alla necessità di promuovere una cittadinanza digitale responsabile e consapevole, volta a fornire strumenti cognitivi e abilità necessari per consentire a ciascun individuo di poter realizzare la propria persona e dar seguito alle proprie attitudini e aspirazioni nell’ambiente virtuale e in relazione alla rapidità con cui le nuove tecnologie stanno evolvendo e impattando sulla quotidianità.

Calando la proposta in esempi pratici emersi dalla ricostruzione e mantenendo il paragone con la circolazione stradale, potremmo pensare di strutturare il percorso abilitante attraverso moduli teorici e simulazioni pratiche sui seguenti profili.

1. Acquisizione di conoscenze in materia di protezione dei dati personali: concetto di confidenzialità, integrità e disponibilità delle informazioni.

2. Acquisizione di conoscenze rispetto ai servizi digitali: liceità dei contenuti.

3. Acquisizione di conoscenze rispetto ai rischi propri della dimensione digitale: sicurezza e governo delle informazioni.

4. Rispetto della vita, dignità, inclusione, non discriminazione, non violenza, e ambiente.

5. Acquisizione di competenze per discernere i contenuti e validare i risultati di processi automatizzati: *fake news*, disinformazione, disinformazione, verifica delle fonti, validazione dei contenuti generati da sistemi IA.

6. Acquisizione elementari conoscenze sul funzionamento di sistemi di IA in caso di emergenza.

7. Acquisizione competenze e conoscenze sui rischi sulla salute fisica e mentale.

8. Acquisizione di competenze per segnalare malfunzionamenti o criticità.

Al pari del patentino, necessario per autorizzare la guida dei ciclomotori, l'adolescente che abbia compiuto gli anni quattordici dovrebbe poter sostenere un esame teorico e uno pratico con personale specializzato e presso enti accreditati. L'esame dovrebbe testare e accertare le capacità e abilità del candidato sia in un ambiente simulato che in scenari reale, al fine di poter accertare la capacità di prevenzione e controllo rispetto a rischi e pericoli: di fatto si tratta di misurare il livello di adeguatezza della capacità di discernimento dell'adolescente rispetto alla possibilità che possa risultare sufficientemente matura per l'utilizzo autonomo dei servizi e prodotti digitali.

3. Non ho l'età, ma... ho il patentino: circolazione del modello e implicazioni sui paradigmi di responsabilità...

La proposta di introdurre il "patentino digitale" per gli adolescenti appare rispondere alle esigenze comuni di completare le iniziative volte a regolamentare il mercato digitale e quello delle nuove tecnologie sia in termini di rapporti tra impresa e consumatori, sia in relazione agli interessi pubblici alla sicurezza e innovazione, con un intervento di carattere culturale capace di guardare all'evoluzione della società che sta vivendo la rivoluzione tecnologica.

Affinché il modello possa trovare concreta applicazione non solo in Italia, ma in una prospettiva transfrontaliera, tuttavia, occorre individuare incentivi e valutare possibili barriere attuative.

A titolo esemplificativo, sul piano istituzionale, dovrebbero essere

forniti incentivi economici per la frequenza dei corsi teorici e delle simulazioni pratiche attraverso misure a sostegno delle famiglie, in modo da garantire la più ampia partecipazione. Non diversamente, fra l'altro, potrebbero essere promossi percorsi analoghi anche per adulti, in ragione delle osservazioni che abbiamo compiuto in ordine alla fluidità del concetto di vulnerabilità digitale, al fine di promuovere un ambiente più sicuro e un utilizzo consapevole degli strumenti di intelligenza artificiale.

Sul piano attuativo, specifiche indicazioni dalle autorità indipendenti dovrebbero poi poter promuovere l'utilizzo del titolo certificato (il patentino digitale o come potrà chiamarsi) come criterio di *accountability* di accompagnamento (ma non sostitutivo) alle altre misure tecniche e/o organizzative che siano ritenute appropriate a seguito delle valutazioni di impatto dall'operatore per l'utilizzo dello specifico strumento da parte di minori di età. Nel capitolo precedente abbiamo altresì rappresentato le potenzialità di individuare un sistema di *enforcement* eventualmente a punti per disincentivare condotte inappropriate.

Sul piano di applicazione transfrontaliera, l'elaborazione di obiettivi comuni di apprendimento e di *standard* di accertamento ben consentirebbero di rendere interoperabile il certificato affinché il patentino possa essere utilizzabile a prescindere dal paese che lo abbia erogato. In questa prospettiva, le iniziative sulla creazione di competenze digitali che abbiamo discusso nel corso della trattazione possono offrire un robusto punto di partenza per poter accelerare il processo di identificazione dei requisiti di accreditamento di iniziative eventualmente attive da ritardare rispetto all'utenza minorenni.

Sul piano della sostenibilità della misura: la revisione periodica delle modalità di erogazione dei programmi e dei contenuti stessi dovrebbe poter far fronte al processo di evoluzione culturale della società nell'era digitale, consentendo anche livelli differenziati, che possano avere un riscontro pratico per l'utilizzatore, rispetto alla disponibilità delle tecnologie utilizzabili.

Le ricadute sul sistema delle responsabilità genitoriali, invero, si rivelano ancor più interessanti. In primo luogo abbiamo ipotizzato che l'introduzione di un percorso formativo obbligatorio per poter fruire dei servizi digitali e prodotti tecnologici in autonomia possa essere *in toto* paragonato alla patente per la guida del ciclomotore, che nulla impatta sull'esercizio delle responsabilità genitoriali, in senso stretto, ma si pone a supporto della responsabilità vicaria ai sensi dell'art. 2048

c.c. e 2054 c.c. innesca, come abbiamo osservato nei precedenti capitoli, un obbligo di assicurare il mezzo con cui l'adulto e/o il minore di età (nella specie patentato) circolano su strada. Di conseguenza, la gestione del rischio dell'utilizzo di servizi e prodotti digitali ben potrebbe aprirsi al mercato assicurativo: la possibilità di introdurre meccanismi di assicurazione della responsabilità civile contro i danni eventualmente causati dall'uso (improprio o colposo) dei servizi della società dell'informazione e delle nuove tecnologie non solo per gli adulti, ma anche (e soprattutto) da parte di giovani utenti, estendendo esplicitamente la copertura delle polizze chiamate "capofamiglia" ⁽⁹⁾ (combinando ad esempio i fattori di rischio e i meccanismi di franchigia) in relazione all'acquisizione o meno del "patentino digitale" appare tutt'altro che peregrina. Oppure, parallelamente all'assicurazione per responsabilità civile automobilistica, potrebbero essere individuate polizze a tutela degli eventuali danni cagionati dall'uso della tecnologia da parte dell'utente, nella specie equiparato al conducente del veicolo, e del titolare della linea per l'erogazione del servizio o del prodotto, *mutatis mutandis* al pari della posizione del proprietario del veicolo ⁽¹⁰⁾.

In secondo luogo, con una prospettiva di più ampio respiro, abbiamo definito alcune condizioni per ricostruire i limiti e i confini della capacità legale di agire rispetto al minore di età, in ragione dell'accertata acquisizione di spazi di autonomia, volti a consentire l'introduzione di formule di emancipazione (*rectius* di disapplicazione della rappresentanza legale del genitore) a condizioni proporzionate all'accertamento dell'acquisizione di competenze e abilità specifiche in ragione di atti che possono considerarsi di ordinaria amministrazione nel dato momento storico.

Abbiamo infine rilevato come principi informatori che regolano la dimensione digitale ben si prestino a fungere da banco di prova rispetto all'attuazione di soluzioni, che possiamo considerare a geometria variabile, volte a indirizzare l'annoso problema legato al peso specifico da

⁽⁹⁾ R. VUORIKARI, S. KLUZER, Y. PUNIE, *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.

⁽¹⁰⁾ Circolano già da tempo, invero, polizze *cyber-risk* per le aziende contro gli attacchi di sicurezza ai sistemi informativi, A. DAMIANI, A. BELLIZZI, M.C. GIUSTINIANI, R. GRECO, *Indagine sulle polizze a copertura cyber risk*, ottobre 2023, Report IVASS pubblicato dalla Divisione Editoria e stampa della Banca d'Italia.

attribuire — caso per caso — alla crescente autonomia degli adolescenti. Abbiamo visto, infatti, come il legislatore UE stesso abbia fornito un segnale evidente, con l'invito ai legislatori nazionali ai sensi dell'art. 8 GDPR ad operare un rinnovato bilanciamento tra il raggiungimento del requisito dell'età anagrafica per poter porre in essere atti giuridici rilevanti e la capacità di fatto di partecipare attivamente e con cognizione di causa ai processi decisionali, a far esprimere direttamente ai soggetti interessati minori di età un consenso libero e valido ai fini del trattamento dei propri dati personali nei servizi della società dell'informazione. In aggiunta abbiamo osservato che non sia dirimente tanto il compimento di una certa soglia di età, ma il fatto che l'adolescente abbia già maturato un bagaglio di conoscenze ed esperienze appropriato per essere in grado (*rectius* capace) di esprimere la propria opinione e gestire i flussi di dati, controllandoli responsabilmente.

Sempre mantenendo il paragone con la circolazione stradale non è un caso che vi siano soglie più basse rispetto al compimento della maggiore età per poter guidare ciclomotori e moto, purché non si raggiunga una certa potenza, anche in questo caso previa acquisizione di competenze teoriche e pratiche specifiche, accertate attraverso un percorso accreditato e certificato che rilasci una idoneità (il patentino per l'appunto).

4. (*Segue*). ... interessi superiori, (in)capacità e dignità del minore di età.

La riflessione sulla dimensione digitale dei diritti dei fanciulli ha infine consentito di arricchire di contenuti categorie giuridiche chiave per la relativa promozione e, non solo, protezione.

In particolare, nel corso della trattazione abbiamo guardato al minore di età, al pari di qualsiasi adulto, in una duplice prospettiva: quella di utente attivo della società dell'informazione e quella di soggetto interessato di informazioni personali trattate attraverso servizi e prodotti digitali. Abbiamo dunque declinato il principio di perseguimento dei *best interests of the child* nello spazio digitale interpretando le diverse istanze di tutela alla luce dei corrispondenti diritti fondamentali del bambino e dell'adolescente. Specialmente laddove il minore abbia un ruolo passivo rispetto allo specifico servizio o prodotto della società dell'informazione (si pensi al fenomeno dello *sharenting*, in cui il figlio subisce le scelte del genitore rispetto alla condivisione di

informazioni che lo riguardano senza che possa partecipare alla decisione, ovvero in caso di profilazione a fini di *marketing*) abbiamo osservato come l'interesse del bambino e dell'adolescente si persegua di pari passo alla protezione dei relativi flussi informativi, attuando i principi di minimizzazione, necessità, liceità affinché conseguenze (anche imprevedibili come *grooming* o manipolazioni) possano impattare sul benessere del soggetto interessato in ragione di una condotta apparentemente innocua, ma probabilmente superficiale rispetto alla valutazione dei rischi, dell'adulto. In questi casi, abbiamo visto come l'approccio dell'interprete (vuoi nelle linee guida delle autorità garanti, vuoi della giurisprudenza) si sia posta in ottica restrittiva, legata a privilegiare, in assenza di effettivi benefici, la protezione della disponibilità, integrità e confidenzialità delle informazioni, mutuando dalla legislazione di settore finalità e strumenti per individuare nel caso concreto la soluzione che esponga — solo se necessario — il minore e i relativi dati ai servizi e prodotti della società dell'informazione, in attuazione del principio di minimizzazione.

Diversamente accade laddove il minore sia l'effettivo utente del servizio o del prodotto: in quel caso le opportunità e i benefici dell'utilizzo vanno a introdurre nuovi elementi nella valutazione, facendo leva non solo sui diritti alla vita privata e familiare, alla protezione dei dati, alla salute, ma anche (e soprattutto) alla promozione delle libertà di esprimere la propria opinione, di associarsi, di imparare e persino di giocare. Laddove il minore di età abbia un ruolo attivo, pertanto, nella società dell'informazione, il perseguimento dei cc.dd. *best interests* si arricchisce di nuove sfumature: l'uso fisiologico dei servizi della società dell'informazione e delle nuove tecnologie porta benessere, occorre tuttavia preservare dall'eventuale uso non appropriato, patologico che vada a compromettere la sicurezza, incolumità e salute fisica e mentale della persona, come osservato nei casi di sfide che inducono alla violenza, odio (dagli esiti anche mortali), cyberbullismo o sviluppo di dipendenze e patologie. Anche in questo scenario gli interessi e diritti da proteggere non si differenziano da quelli degli utenti adulti, se non per il fatto che la protezione del minore di età riguarda la necessità di preservare il relativo benessere nella costruzione dell'adulto del domani e, dunque, del pensiero critico, delle abilità e delle conoscenze ovvero della persona in formazione che ancora non abbia completato l'acquisizione di strumenti cognitivi, emotivi, e relazionali per gestire autonomamente i propri interessi. In questo scenario, assumono particolare rilievo i principi di non discriminazione e

inclusività, che — declinati con le lenti del perseguimento del *best interest* — portano a stimolare e sperimentare forme di partecipazione ai processi decisionali e a cogliere con responsabilità le sfide della società, rendendo il bambino prima — e progressivamente l'adolescente — un utente sempre più autonomo nella fruizione di servizi e prodotti digitali. Abbiamo collegato inoltre l'esercizio dei diritti individuali alla realizzazione della persona nel contesto comunitario: il che significa proiettare la promozione del singolo come cittadino informato, consapevole, istruito, etc., pronto a svolgere il proprio ruolo nella (e per la) realtà in cui vive.

Di conseguenza, ritorna la lettura della dignità della persona alla luce non soltanto del binomio protezione-incapacità. Il minorenne non è solo destinatario o utilizzatore finale passivo delle nuove tecnologie, ma nello spazio digitale esercita i propri diritti in quanto può esprimersi, associarsi, comunicare, imparare, giocare, conoscere, formarsi, etc. Seppur condizionato alla soddisfazione di certi requisiti per poter accedere ai servizi e prodotti (includendo fra questi l'accertamento dell'acquisizione di competenze e abilità attraverso il proposto patentino digitale), seppur con possibili limitazioni nel modo di esercitare le facoltà derivanti dalla propria posizione (nei contenuti, nei tempi di fruizione ad esempio), la declinazione della dignità della persona alla luce del perseguimento del benessere del bambino e dell'adolescente non giustifica (più) l'esclusione perché incapace di poter fruire servizi e prodotti autonomamente derivante dal mancato compimento della maggiore età.

Più che di (in)capacità di agire appare opportuno riformulare la posizione del minore di età alla luce del principio dei *best interests of the child* come mezzo per attuare la dignità della persona. Occorre accompagnare la protezione-incapacità a meccanismi di promozione-capacità condizionata alla soddisfazione di quei requisiti che possono rendere il minorenne progressivamente più autonomo dal genitore. Ciò vale nella circolazione stradale, come osservato, e, *mutatis mutandis*, nell'ambiente digitale, dove tali requisiti devono poter dar evidenza dei seguenti risultati: *i*) dell'acquisizione di un bagaglio esperienziale e di maturità psico-fisica sufficiente a definire il completamento del passaggio dal livello di immaturità del bambino a quello dell'adolescente (*i.e.* maturità psico-cognitiva); *ii*) di aver acquisito competenze e conoscenze specifiche attraverso idonea istruzione ed educazione, possibilmente certificata al porre in essere atti giuridici rilevanti in un determinato settore (*i.e.* alfabetizzazione); *iii*) dell'ambito di applicazione di

una consapevole supervisione da parte di coloro che esercitino le responsabilità genitoriali in sostituzione della legale rappresentanza, laddove vi siano meccanismi (ad esempio attraverso l'introduzione di obblighi di copertura assicurativa che possano garantire l'operare di meccanismi risarcitori efficaci in caso di patologia dei rapporti tra consociati); *iv*) di poter valutare tutti gli ulteriori elementi necessari per garantire il perseguimento degli interessi superiori dei minori nelle scelte adottate (attraverso gli obblighi di *due diligence* e valutazione di impatto per i prestatori di servizi digitali e fornitori e utilizzatori dei sistemi di IA).

Calando la proposta nell'ambito dell'art. 2 c.c., comma 2, potrebbe essere eliminato il riferimento all'eccezione relativa al compimento di anni 18 "*in materia di capacità a prestare il proprio lavoro*", lasciando aperta la possibilità per il legislatore di disciplinare con leggi speciali forme di capacità condizionata in virtù di una lettura evolutiva della dignità della persona e dei diritti fondamentali in una società che non può proteggere dai rischi senza promuovere conoscenza, consapevolezza e abilità per tutte le persone, comprese quelle più giovani.

La capacità condizionata dell'utente minorenne che proponiamo è dunque necessariamente connotata da flessibilità e duttilità, in quanto subordinata a percorsi formativi abilitanti a determinate funzioni e alle sfide che le nuove tecnologie porteranno nei prossimi anni.

Il compito della cultura è proprio quello di garantire che la "tecnica" continui a contribuire alla promozione della dignità e degli altri diritti fondamentali di tutti i cittadini attraverso meccanismi di tutela a geometria variabile che diano voce alle diverse posizioni. Ciò è possibile solo attraverso un processo di evoluzione culturale, capace di rendere la dimensione digitale alla portata di tutti (nessuno escluso), dove consentire di realizzare la propria persona al pari della dimensione fisica, senza limitare la conformità etico-giuridica a un semplice scenario in cui servizi e prodotti sono fruibili solo previo adempimento ad obblighi, previsti da interventi legislativi di settore, ovvero derivanti dal "diritto scritto" ⁽¹¹⁾.

⁽¹¹⁾ "Il diritto scritto offre all'interprete palestre sconfinare per la creazione di un diritto imprevedibile", così R. SACCO, *Il diritto muto*, cit., p. 140.

BIBLIOGRAFIA

- M. ALBERTSON FINEMAN, *The vulnerable subject: Anchoring equality in the human condition*, in *Yale Journal of Law & Feminism*, 2008, 20, 1 s.
- C. ASHRAF, *Exploring the impacts of artificial intelligence on freedom of religion or belief online*, *The International Journal of Human Rights*, 2022, 26:5, 757-791, doi: 10.1080/13642987.2021.1968376.
- G. ALPA, *I contratti del minore. Appunti di diritto comparato*, in *I Contratti*, 2004, p. 520 ss.
- L. ANTONIOLLI, F. CORTESE, E. IORIATTI, B. MARCHETTI (a cura di), *Trento e la comparazione giuridica: voci, esperienze, riflessioni: dalla testimonianza di Rodolfo Sacco e Mauro Cappelletti*, 2024, Edizione Scientifica.
- B. V. ALSENOY, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, Intersentia, 2019.
- AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *Il diritto all'ascolto delle persone di minore età in sede giurisdizionale*, 2020, <https://www.garanteinfanzia.org/sites/default/files/ascolto-minorenni-procedimenti-giurisdizionali.pdf>.
- AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *Geronimo Stilton. Alla scoperta del mondo digitale*, realizzato dall'Agia in collaborazione con Piemme - Mondadori Libri, 2022, https://www.garanteinfanzia.org/sites/default/files/2022-05/EducazioneAlDigitale_WEBok.pdf.
- AUTORITÀ GARANTE PER L'INFANZIA E L'ADOLESCENZA, *Manifesto dei bambini sui diritti in ambiente digitale*, 17.3.2023, disponibile a questo indirizzo: <https://www.garanteinfanzia.org/manifesto-dei-bambini-sui-diritti-ambiente-digitale>.
- O. BAR-GILL-O. BEN-SHAHAR, *Misprioritized Information: A Theory of Manipulation*, *J. Leg. Studies*, 52, 2.
- V. BARBA, *Autonomia progressiva e miglior interesse della persona minore di età*, in *Dir. Succ e fam.*, 2023, p. 441 ss.
- R. BINNS, M. VEALE, *Is that your final decision? Multi-stage profiling, selective effects, and Article 22 of the GDPR*, in *International Data Privacy Law*, Volume 11, Issue 4, November 2021, p. 319 <https://doi.org/10.1093/idpl/ipab020>.
- O. BEN-SHAHAR - A. PORAT, *Personalized Law. Different Rules for Different People*, Oxford, 2021.
- O. BEN-SHAHAR & C. E. SCHNEIDER, 'The Failure of Mandated Disclosure' (2017) 2017 *Actual Probs Econ & L* 146.
- O. BEN-SHAHAR, 'The Myth of the 'Opportunity to Read' in Contract Law' (2009) 5(1) *European Review of Contract Law* 1.

- K. BOELE-WOELKI, *Common Core and Better Law in European Family Law*, Intersentia, 2005.
- J.C. BUBLITZ, *Novel neurorights: From nonsense to substance*, *Neuroethics* 2022;15(1):7.
- A. BUCCELLI (a cura di), *Identità e salute del minore. Problematiche attuali*, Pisa, 2021.
- F.D. BUSNELLI, *Capacità ed incapacità di agire del minore*, in *Dir. fam.*, 1982, p. 61 ss.
- F.D. BUSNELLI, *La dimensione della fragilità lungo il percorso della vita umana*, in *Nuovo diritto civile*, 2016.
- F.D. BUSNELLI, *Le alternanti sorti del principio di dignità della persona umana*, in *Riv. dir. civ.*, 2019, p. 1071 ss.
- S. CACACE, *Autodeterminazione in salute*, Torino, 2017.
- CAFAGGI F., MICLKITZ H., *Enforcement pubblico e privato nel diritto dei consumatori: lineamenti per una comparazione comparata del sistema statunitense ed europeo*, in M. MAUGERI e A. ZOPPINI, *Funzioni del diritto privato e tecniche di regolazione del mercato - Le funzioni della responsabilità civile* Mulino, Bologna, 2009.
- G. CALABRESI-P. BOBBIT, *Le scelte tragiche*, Giuffrè, 2006.
- V. CALDERAI, *Consenso informato*, in *Enc. dir.*, Ann., Milano, 2015.
- H. CAMPBELL, *When religion meets new media* Routledge, 2010, L. KONG, *Religion and Technology: Refiguring Place, Space, Identity and Community*, in *Area*, Vol. 33, No. 4 (Dec., 2001), p. 404 ss.
- M. CANTERO GAMITO-H. W. MICKLITZ, *Too much or too little? Assessing the Consumer Protection Cooperation (CPC), Network in the protection of consumers and children on TikTok* (BEUC, 17-02-23) https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-018_Assessing_CPC_Network_in_the_protection_of_consumers_and_children_on_TikTok-Report.pdf.
- G. CAPILLI, *La capacità negoziale dei minori. Analisi comparata e prospettive di riforma*, Torino, 2012, p. 12 ss.
- M. CASTELLS, *The Rise of the Network Society*, The Information Age: Economy, Society and Culture Vol. I., 1996, Cambridge, MA; Oxford, UK: Blackwell, Id., *The Power of Identity*, The Information Age: Economy, Society and Culture Vol. II., 1997, Cambridge, MA; Id., *End of Millennium*, The Information Age: Economy, Society and Culture, Vol. III., 1998.
- A. CAVOUKIAN, *Privacy by design: the definitive workshop. A foreword by Ann Cavoukian*, Ph.D. IDIS 3, 247-251 (2010). <https://doi.org/10.1007/s12394-010-0062-y>.
- A. CHANDER, M. E. KAMINSKI, W. MCGEVERAN, *Catalyzing Privacy Law*, 105 Minnesota L. Rev. 1733 (April 2021).
- V. CHARISI, S. CHAUDRON, R. DI GIOIA, R. VUORIKARI, M. ESCOBAR-PLANAS, I. SANCHEZ, E. GOMEZ, *Artificial Intelligence and the Rights of the Child Towards an Integrated Agenda for Research and Policy*, JRC Report, Brussels, 2022, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC127564/JRC127564_01.pdf.
- M. CINQUE, *Il minore contraente. Contesti e limiti della capacità*, Padova, 2007.

- T. CHEN, J. OU, G. LI, H. LUO, *Promoting mental health in children and adolescents through digital technology: a systematic review and meta-analysis*. Front Psychol. 2024.
- M. CINQUE, *Il minore contraente. Contesti e limiti della capacità*, Padova, 2007.
- A. COLE, *All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique*, Critical Horizons, 2016, 17(2), 260-277.
- G. COMANDÉ, (a cura di), *Elgar Encyclopedia of Law and Data Science*, 2022.
- G. COMANDÉ, *Unfolding the Legal Component of Trustworthy AI: A Must to Avoid Ethics Washing*, in *Annuario di Diritto Comparato e di Studi Legislativi*, 2020, p. 29 s.
- G. COMANDÉ-G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali*, IlSole24ore, 2018.
- G. COMANDÉ-G. PONZANELLI (a cura di), *Scienza e diritto nel prisma del diritto comparato*, Torino, 2004.
- M.I. CORNEJO-PLAZA, R. CIPPITANI, V. PASQUINO, *Chilean Supreme Court ruling on the protection of brain activity: neurorights, personal data protection, and neurodata*. Front Psychol. 2024 Feb 27;15:1330439. doi: 10.3389/fpsyg.2024.1330439. PMID: 38476399; PMCID: PMC10929545.
- C. CREA A. DE FRANCESCHI (Eds), *The New Shapes of Digital Vulnerability in European Private Law*, Nomos, 2024.
- B. DEL LUCCHESI, S. PARRAVICINI, S. FILOGNA, G. MANGANI, E. BEANI, MC DI LIETO, A. BARDONI, M. BERTAMINO, M. PAPINI, C. TACCHINO, F. FEDELI, G. CIONI, G. SGANDURRA AND THE ITALIAN NEUROSCIENCE AND NEUROREHABILITATION NETWORK (2024) *The wide world of technological telerehabilitation for pediatric neurologic and neurodevelopmental disorders - a systematic review*, in *Front. Public Health* 12:1295273. doi: 10.3389/fpubh.2024.1295273.
- N. DETHLOFF, K. KAESLING, L. SPECHT-RIEMENSCHNEIDER (a cura di) *Families and New Media*. Springer, Wiesbaden, 2023, https://doi.org/10.1007/978-3-658-39664-0_9.
- G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022.
- W. DE SANTANA, A. L. Y ARCHEGAS, J. GABRIEL, *La protección de niños y adolescentes en las plataformas digitales: Avances en el tema en Brasil. Agenda Estado de Derecho*, 2023/12/20 Disponible en: <https://agendaestadodederecho.com/la-proteccion-de-ninos-y-adolescentes-en-las-plataformas-digitales-avances-en-brasil>.
- F. DI PORTO-A. EGBERS, *The collective welfare dimension of dark patterns regulation*, in *Europeal Law Journal*, 2024, vol 29, p. 114 s.
- R. DOSHI, O.P. HAUSER, *Generative AI enhances individual creativity but reduces the collective diversity of novel content*, Sci. Adv.10, eadn5290 (2024), DOI:10.1126/sciadv.adn5290.
- R. DUCATO, H. HAPIO, M. HAGAN, M. PALMIRANI, S. PASSERA, A. ROSSI, *The Legal Design Manifesto v.1*, 2018, <https://www.legaldesignalliance.org>.
- L. EUM LEE, *Metaphor analysis on pre-service early childhood teachers' conception of AI (Artificial Intelligence) education for young children*, Thinking Skills and Creativity, 2024, Elsevier, Doi: 10.1016/j.tsc.2023.101455.

- EU COMMISSION, *Digital4Development: mainstreaming digital technologies and services into EU Development Policy*, Brussels, 2.5.2017 SWD(2017) 157 final.
- J. FAIRFIELD-C. ENGEL, *Privacy as a Public Good*, 2015, 65 Duke Law Journal, 385.
- A. FIGONE, *La violenza. Artt. 1434-1439 Codice Civile Commentato*, Giuffrè, 2005.
- G. FINOCCHIARO, *La proposta di Regolamento sull'Intelligenza Artificiale: il modello Europeo basato sulla gestione del rischio*, Dir. Informazione e dell'informatica, 2022, p. 303 ss.
- G. FINOCCHIARO, L. BALESTRA, M. TIMOTEO (a cura di), *Major Legal Trends in the Digital Economy. The Approach of the EU, the US and China*, Bologna, 2022.
- K. O' FLAHERTY, ChatGPT-4o Is Wildly Capable, But It Could Be A Privacy Nightmare, Forbes, 17.5.2024, <https://www.forbes.com/sites/kateoflahertyuk/2024/05/17/chatgpt-4o-is-wildly-capable-but-it-could-be-a-privacy-nightmare/>.
- L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.
- L. GATT, *Legal anthropocentrism between nature and technology: the new vulnerability of human beings*, (2022) 1 EJPLT, 15-26.
- L. GATT, I. CAGGIANO, *Consumers and Digital Environments as a Structural Vulnerability Relationship* (2022) 2 EJPLT, 8-16. DOI: <https://doi.org/10.57230/EJPLT222LGIAC>.
- A. GENTILI, *Crisi delle categorie e crisi degli interpreti*, in Riv. dir. civ., 4, 2021, p. 653.
- R. GIARDA, J. LIOTTA, G. RINDI, *Vita quotidiana del minore online. Tra esigenze di tutela e limiti tecnologici*, MediaLaws, 183 ss.
- F. GIARDINA, *La condizione giuridica del minore*, Napoli, 1984.
- F. GIARDINA, *Per un'indagine sulla responsabilità civile nella famiglia. L'art. 129-bis del codice civile*, Pisa, ETS, 1999.
- F. GIUSTOZZI, *Atti giuridici e capacità di agire*, Edizioni Scientifiche Italiane, 2021.
- G. GORLA, *Diritto comparato e diritto comune europeo*, Milano, 1981.
- M. GRAZIADEI, *Comparative Law, Transplants, and Receptions*, in REIMANN, MATHIAS, AND REINHARD ZIMMERMANN (eds), *The Oxford Handbook of Comparative Law*, 2nd edn, Oxford Handbooks 2019, p. 456 ss.
- B. GREEN, *The Flaws of Policies Requiring Human Oversight of Government Algorithms*, in *Computer Law & Security Review*, Volume 45, 2022, <https://doi.org/10.1016/j.clsr.2022.105681>.
- L. GREEN, D. HOLLOWAY, K. STEVENSON, T. LEAVER, L. HADDON (eds), *The Routledge Companion to Digital Media and Children*, London, UK: Routledge, 2020.
- P. GROSSI, *Scienza giuridica italiana. Un profilo storico 1860-1950-2000*, Milano, 2000.
- P. GUARDA-G. BINCOLETTI, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023.

- R. HAWKINS, *Standards for Communication Technologies: Negotiating Institutional Biases in Network Design*, in R. MANSELL-R. SILVERSTONE (a cura di), *Communication by Design: The Politics of Information and Communication Technologies*, 1996, Oxford: Oxford University Press, p. 157 ss.
- N. HELBERGER, M. SAX, J. STRYCHARZ, H.-W. MICKLITZ, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, in *Journal of Consumer Policy*, 2022, 45:175-200.
- C. HELLAND, *Virtual Religion: A Case Study of Virtual Tibet*, Oxford Handbooks, 2015.
- H. HOLMARSÐÓTTIR, *The Digital Divide: Understanding Vulnerability and Risk in Children and Young People's Everyday Digital Lives*. In: Holmarsdottir, H., Seland, I., Hyggen, C., Roth, M. (eds) *Understanding The Everyday Digital Lives of Children and Young People*, 2024, Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-46929-9_3.
- W. HOLMES-I. TUOMI (2022), *State of the art and practice in AI in education*. *European Journal of Education*, 57, pp. 542.
- G. HOWELLS, H.W. MICKLITZ, T. WILHELMSSON, *European Fair Trading Law. The Unfair Commercial Practices Directive*, London, 2006.
- K. HU, *ChatGPT sets record for fastest-growing user base - analyst note*, 2 febbraio 2023, Reuters, in <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01..>
- M. IENCA, R. ANDORNO, *Verso nuovi diritti umani nell'era delle neuroscienze e delle neurotecnologie*, Life Sciences, Society and Policy, 2017, 13, (1), pp. 5.
- C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021.
- N. IRTI, *Significato giuridico dell'effettività*, Napoli, 2009, p. 13 ss.
- N. IRTI-E. SEVERINO, *Dialogo su diritto e tecnica*, Laterza, 2001.
- L. JASMONTAITE-P. DE HERT, *The EU, Children under 13 Years, and Parental Consent: A Human Rights Analysis of a New, Age-Based Bright-Line for the Protection of Children on the Internet* (2014) 5 *International Data Privacy Law* 20 ss.
- NS. JECKER-A. KO (2023). *Are Neurorights Global?* *AJOB Neuroscience*, 14(4), 369-371 <https://doi.org/10.1080/21507740.2023.2257151>.
- M.E. KAMINSKI, *Understanding Transparency in Algorithmic Accountability*, in Barfield W, ed. *The Cambridge Handbook of the Law of Algorithms*. Cambridge Law Handbooks. Cambridge University Press; 2020:121-138.
- D. KER-E. MAZZINI (2020), "Perspectives on the value of data and data flows", *OECD Digital Economy Papers*, No. 299, OECD Publishing, Paris, <https://doi.org/10.1787/a2216bc1-en>.
- C. KUNER ET AL. (a cura di), *The EU General Data Protection Regulation (GDPR): A Commentary*, New York, 2020; online edn, Oxford Academic.
- E. LAMARQUE, *Prima i bambini. Il principio dei best interests of the child nella prospettiva costituzionale*, FrancoAngeli, Milano, 2016.
- G. LAZCOZ, P. DE HERT, *Humans in the GDPR and AIA governance of automated and algorithmic systems. Essential pre-requisites against abdication responsibilities*, in *Computer & Law Security Review*, 2023, 50, 105833, 7-8.

- T. LEAVER, *Balancing privacy: sharenting, intimate surveillance, and the right to be forgotten*, In: L. GREEN, D. HOLLOWAY, K. STEVENSON, T. LEAVER, L. HADDON (a cura di), *The Routledge Companion to Digital Media and Children*, London, UK: Routledge; 2020. pp. 235-44; G. OUVREIN, K. VERSWIJVEL, *Sharenting: parental adoration or public humiliation? A focus group study on adolescents' experiences with sharenting against the background of their own impression management*, *Child Youth Serv Rev.* 2019.
- C. LI, B. PALANISAMY, *Privacy in Internet of Things: From Principles to Technologies*, in *IEEE Internet of Things Journal*, 2019, p. 488 s.
- E. LIEVENS-V. VERDOODT, *Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation* (2018) 34(2) *Computer Law & Security Review* 269.
- S. LIGTHART, M. IENCA, G. MEYNEN ET AL. *Minding Rights: Mapping Ethical and Legal Foundations of 'Neurorights.'* *Cambridge Quarterly of Healthcare Ethics.* 2023;32(4):461-481. doi:10.1017/S0963180123000245.
- S. LIGTHART, T. DOUGLAS, C. BUBLITZ, T. KOIJMANS, G. MEYNEN, *Forensic brain-reading and mental privacy in European Human Rights Law: Foundations and challenges.* *Neuroethics* 2021;14(2):191-203.
- S. LIVINGSTONE, E. LIEVENS, J. CARR, *Handbook for policy makers on the rights of the child in the digital environment*, CoE - Strasborug, 2021, <https://rm.coe.int/handbook-for-policy-makers-on-the-rights-of-the-child-in-the-digital-e/1680a069f8>.
- V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: a revolution that will transform how we live, work, and think*, Mariner Books, New York, 2014.
- G. MALGIERI-G. COMANDÉ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law* 7, no. 4, 2017: 243-65, <https://doi.org/10.1093/idpl/ix019>.
- G. MALGIERI, *Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations*, in *Computer Law & Security Review*, Volume 35, Issue 5, 2019, 105327, <https://doi.org/10.1016/j.clsr.2019.05.002>.
- G. MALGIERI, *Vulnerability and Data Protection Law*, Oxford University Press, April 2023.
- A. MANSFERRER, E. GARCIA-SÁNCHEZ (a cura di), *Human Dignity of the Vulnerable in the Age of Rights*, Dordrecht: Springer, 2016.
- A. MANTELERO, *Children Online and the Future EU Data Protection Framework: Empirical Evidences and Legal Analysis* (2016) 2 *International Journal of Technology Policy and Law* p. 169-81.
- A. MANTELERO-M. S. ESPOSITO, *An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems*, in *Computer Law & Security Review*, Volume 41, 2021, 105561, ISSN 0267-3649, <https://doi.org/10.1016/j.clsr.2021.105561>.
- R. MARGOLIS, *Forays into a Digital Yiddishland: Secular Yiddish in the Early Stages of the Coronavirus Pandemic.* *Contemp Jew.* 2021;41(1):71-98. doi: 10.1007/s12397-021-09379-x. Epub 2021 Jul 20. PMID: 34305202; PMCID: PMC8290379.

- S. MATHIAZHAGAN-K. LA FORS, *Children's right to participation in AI: Exploring transnational co-creative approaches to foster child-inclusive AI policy and practice*. Info. Pol. 28, 1 (2023), 141-153.
- A. MIRANDA, *Lo "stingimento" delle regole giuridiche tra diritti e limiti nell'era dei flussi migratori e della crisi delle nazioni*, in *Cardozo El. Law Bull*, 2018, 11 ss.
- A. MIRANDA (a cura di), *Diritto e tradizione. Circolazione, decodificazione e persistenza delle norme giuridiche*, Palermo, 2004.
- C. NYAMUTATA, *Childhood in the Digital Age: A Socio-Cultural and Legal Analysis of the UK's Proposed Virtual Legal Duty of Care* (2019) 27:4 Int'l JL & Info Tech 311.
- OECD, *Children in the digital environment*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389?_ga=2.138548851.1597661473.1707343531-2141752145.1706178830.
- G. PALMERI, *Diritti senza poteri. La condizione giuridica dei minori*, Napoli, 1994.
- S. PANUNZIO, *Età*, in *Enciclopedia giuridica Treccani*, vol. XIII, Roma, 1989, pp. 1 ss.
- R. PARDOLESI-A. DAVOLA, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i 'dark pattern'): parallele convergenti?* cc.dd. *dark patterns*, Foro it., 2021, c. 338.
- F. PEDRINI, *Santi Romano e l'interpretazione giuridica. Appunti per una riflessione sul "metodo" nel diritto pubblico*, *Jura Gentium*, XV (2018), 2, p. 79 ss.
- M.P. PIGNALOSA, *Contratti a distanza e recesso del consumatore*, Milano, 2016, 253 ss.
- A. PIZZORUSSO, *L'apporto della comparazione alla scienza*, Milano, 1980.
- D. POLETTI, *Gli intermediari dei dati* (2022) 1 EJPLT, 45-56. DOI: <https://doi.org/10.57230/EJPLT221DP>.
- O. POLLICINO, *Verso il Digital Services Act: problemi e prospettive. Presentazione del simposio*, MediaLaws, 2020.
- L. PROVENZI, S. GRUMI, R. BORGATTI (a cura di), *Family-Centered Care in Childhood Disability*, 2023, Springer, Cham. https://doi.org/10.1007/978-3-031-34252-3_5.
- A. QUERCI, *L'incapacità naturale all'esame della giurisprudenza: un contrasto fra massime?*, in *Contratto e impresa*, 2012, p. 1466 s.
- P. RESCIGNO, *Incapacità naturale e adempimento*, Napoli, 1982.
- G. RESTA, *Diritti della personalità: problemi e prospettive*, in *Dir. dell'informazione e dell'informatica*, 2007, p. 1043 ss.
- G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista Trimestrale di Diritto Pubblico*, 2022, p. 975.
- F. RESTA, *Consenso del minore in relazione ai servizi della società dell'informazione*, Commentario al Codice della Privacy, R. Sciaudone (a cura di), Pacini Giuridica, 2023.
- J. RIFKIN, *The Age of Access: The New Culture of Hypercapitalism*, Penguin Putnam Inc, 2001.
- P. RESCIGNO, *Capacità di agire*, in *Novissimo digesto italiano*, vol. II, Torino, 1988, p. 862.

- P. RESCIGNO, *Capacità di agire*, in *Digesto discipline privatistiche*, Sezione civile, vol. II, Torino, 1988, pp. 213 s.
- S. RIGAZIO, *L'empowerment del minore nella dimensione digitale*, Mucchi, 2024.
- S. RODOTÀ, *Il problema della responsabilità civile*, Milano, 1964.
- S. RODOTÀ, *Privacy e costruzione della sfera privata*, in *Tecnologie e diritti*, Bologna, 1999.
- S. RODOTÀ, *Il diritto di avere diritti*, Roma, 2015.
- J. RUOHONEN, S. MICKELSSON, *Reflections on the Data Governance Act*, DISO 2, 10 (2023) <https://doi.org/10.1007/s44206-023-00041-7>.
- C. RUPERTO, *Età (dir. priv.)*, in *Enciclopedia del diritto*, vol. XVI, Milano, 1967, pp. 85 s.
- R. SACCO, *Circolazione e mutazione dei modelli giuridici*, in *Dig. Disc. Priv.*, Sez. civ., v. II, Torino, 1988, 365 ss.
- R. SACCO, *Il diritto muto*, Il Mulino, 2015.
- R. SACCO, *Che cos'è il diritto comparato*, Milano, 1992.
- M.R. SAULLE, *Codice internazionale dei diritti del minore*, ESI, Napoli, 1992.
- V. SCALISI, *Ermeneutica della dignità*, Milano, 2018.
- V. SCALISI, *Superiore interesse del minore ovvero il fatto come diritto*, in *Riv. dir. civ.*, 2018, I, p. 407.
- D. SHARMA, L. BHAGAT, S. SHARMA, *Regulating Children's Personal Data Protection in India: No Child's Play*. Development (2024). <https://doi.org/10.1057/s41301-024-00402-w>.
- W. SCHRAMA, M. FREEMAN, N. TAYLOR, M. BRUNING (a cura di), *International Handbook on Child Participation in Family Law*, Cambridge-Antwerp-Chicago, 2021.
- A. SESTINO, A. KAHLAWI, A. DE MAURO, *Decoding the data economy: a literature review of its impact on business society and digital transformation*, in *European Journal of Innovation Management*, 2023, doi: <https://www.emerald.com/insight/content/doi/10.1108/EJIM-01-2023-0078/full/html>.
- R. SENIGAGLIA, *Minore età e contratto*, Torino, 2021.
- C. SGANGA, *Is There Still a Policy Agenda for EU Copyright Law?* (2023) *International Review of Intellectual Property and Competition Law*, 54, pp. 1407-1417.
- C. SGANGA, *Limiti e limitazioni al diritto d'autore nel nuovo EU Data Package: alla ricerca del sistema perduto*, AIDA, 2023, p. 338 ss.
- J. SHAHIN-M. FINGER, *The History of a European Information Society: Shifts from governments to governance*, in J. TUBTIMHIN-R. PIPE (a cura di), *Global e-Governance: Advancing governance through innovation and leadership*, Amsterdam, IOS Press, 2009, Global E-Governance Series, Vol. 2, 62-83.
- J. SOLER GARRIDO, D. FANO YELA, C. PANIGUTTI, H. JUNKLEWITZ, R. HAMON, T. EVAS, A. ANDRÉ, S. SCALZO, *Analysis of the preliminary AI standardisation work plan in support of the AI Act*, EUR 31518 EN, Publications Office of the European Union, Luxembourg, 2023, ISBN 978-92-68-03924-3, doi:10.2760/5847, JRC132833.
- P. STANZIONE, *Data Protection and Vulnerability*, 2020, *Eur. J. Privacy L. & Tech.* 9.

- K.K. SMITH, V. BLANES-VIDAL, E.S. NADIMI, U. RAJENDRA ACHARYA, *Emotion recognition and artificial intelligence: A systematic review (2014-2023) and research recommendations*, in *Information Fusion*, Volume 102, 2024, 102019, ISSN 1566-2535, <https://doi.org/10.1016/j.inffus.2023.102019>.
- L. TAFARO, *L'età per l'attività*, Napoli, 2003, p. 36 ss.
- J. TOBIN, *The UN Convention on the Rights of the Child: A Commentary*, Oxford Commentaries on International Law, 2019.
- E. TOSI, *La tutela dei consumatori in Internet e nel commercio elettronico*, Milano, 2012.
- M. TRENGOVE, E. KAZIM, D. ALMEIDA, A. HILLIARD, S. ZANNONE, E. LOMAS, *A critical review of the Online Safety Bill*, *Patterns* (N Y). 2022 Jun 24;3(8):100544. doi: 10.1016/j.patter.2022.100544. PMID: 36033594; PMCID: PMC9403395.
- Z. VAGHRI, J. ZERMATTEN, G. LANSDOWN, R. RUGGIERO (eds), *Monitoring State Compliance with the UN Convention on the Rights of the Child. Children's Well-Being: Indicators and Research*, 2022, vol. 25. Springer, Cham. https://doi.org/10.1007/978-3-030-84647-3_12.
- S. VAN DER HOF-E. LIEVENS, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR* (2018) 23 *Communications Law* 33.
- S. VAN DER HOF, *I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World* (2017) 34(2) *Wisconsin International Law Journal*, p. 409 s.
- V. VARANO, *Alessandro Pizzorusso e la comparazione*, in *Diritto pubblico comparato ed europeo*, 2017, p. 285.
- S.C. VESTERGAARD (ed.) *Encyclopedia of Bullying*, Nova, 2020.
- A. VIGORITO, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, *MediaLaws*, 2023, <https://www.medialaws.eu/rivista/sul-crinale-tra-data-altruism-e-social-scoring-esperienze-applicative-della-sequenza-dati-algoritmi-nel-nuovo-contesto-regolatorio-europeo/>.
- A. VON ARNAULD, K. DER DECKEN, M. SUSI (a cura di) *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric*. Cambridge: Cambridge University Press; 2020:404-12.
- R. VUORIKARI, S. KLUZER, Y. PUNIE, *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48883-5, doi:10.2760/490274, JRC128415.
- VV.AA. *Anthropological Perspectives on the Religious Uses of Mobile Apps*, Springer, 2019.
- A. WATSON, *Legal Transplants. An Approach to Comparative Law*, Edinburgh, 1974, and Athens 1993.
- H. WEIR, *Children's autonomous mobility and their well-being*, *Wellbeing, Space and Society*, Volume 4, 2023, 100134, ISSN 2666-5581, <https://doi.org/10.1016/j.wss.2023.100134>.

- K. WEITZ, D. SCHILLER, R. SCHLAGOWSKI, ET AL. *"Let me explain!": exploring the potential of virtual agents in explainable AI interaction design*. J Multimodal User Interfaces 15, 87-98 (2021) <https://doi.org/10.1007/s12193-020-00332>, A. SIMONCINI, *L'algoritmo incostituzionale, intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, 2019, p. 63 s.
- A.C. WITT, *The Digital Markets Act: Regulating the Wild West*, (2023), 60, Common Market Law Review, Issue 3, pp. 625-666, <https://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/60.3/COLA2023047>.
- P. ZATTI, *Brevi note sull'interpretazione della legge n. 219 del 2017*, in *L.N.G.C.C.*, 2019, p. 3 ss.
- V. ZENO-ZENCOVICH, *Informatica ed evoluzione del diritto*, in *Il diritto dell'informazione e dell'informatica*, fasc. 1, 2003, p. 89 ss.
- V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2018, p. 37.
- V. ZENO-ZENCOVICH, *Artificial intelligence, natural stupidity and other legal idiocies*, *MediaLaws*, 2024.
- L. ZHANG, K. KOLLNIG, *Theory and practice: the protection of children's personal information in China*, in *International Data Privacy Law*, Volume 14, Issue 1, February 2024, p. 37 ss., <https://doi.org/10.1093/idpl/ipad017>.
- Y. ZIHAN ET AL., *NaCanva: Exploring and Enabling the Nature-Inspired Creativity for Children*, *Proceedings of the ACM on human-computer interaction* 7.MHCI (2023): 1-25.
- S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019, New York, Public Affairs.

Dallo studio comparatistico del frammentato quadro normativo in materia di dati e innovazione tecnologica, sorge l'esigenza comune di bilanciare misure volte a prevenire e mitigare rischi derivanti dall'uso di servizi e prodotti digitali da parte di utenti minori di età, rispetto alle opportunità – senza precedenti – di crescita e partecipazione ai processi decisionali.

Definito il paradigma di protezione affinché l'ambiente digitale risulti sicuro e affidabile per tutti gli utenti e – a maggior ragione – per i bambini, l'analisi suggerisce una nuova interpretazione dell'istituto dell'(in)capacità del minore di età, basata sulla combinazione di una pluralità di fattori suscettibili di rendere valutabile la capacità di discernimento (*i.e.* l'idoneità o meno) dell'adolescente ad esercitare in misura progressivamente più autonoma i propri diritti fondamentali nella dimensione digitale.

DENISE AMRAM è ricercatrice *senior* di diritto privato comparato presso la Scuola Superiore Sant'Anna di Pisa.

€ 36,00
024226260

ISBN 978-88-28-87776-9



9 788828 877769