



Freedom, Security & Justice:
European Legal Studies

Rivista giuridica di classe A

2026, n. 2

EDITORIALE
SCIENTIFICA



DIRETTRICE

Angela Di Stasi

Ordinario di Diritto Internazionale e di Diritto dell'Unione europea, Università di Salerno
Titolare della Cattedra Jean Monnet 2017-2020 (Commissione europea)
"Judicial Protection of Fundamental Rights in the European Area of Freedom, Security and Justice"

CONSIGLIO SCIENTIFICO

Giandonato Caggiano, Ordinario f.r. di Diritto dell'Unione europea, Università Roma Tre
Sergio Maria Carbone, Professore Emerito, Università di Genova
Roberta Clerici, Ordinario f.r. di Diritto Internazionale privato, Università di Milano †
Nigel Lowe, Professor Emeritus, University of Cardiff
Paolo Mengozzi, Professore Emerito, Università "Alma Mater Studiorum" di Bologna - già Avvocato generale presso la Corte di giustizia dell'UE
Massimo Panebianco, Professore Emerito, Università di Salerno
Nicoletta Parisi, Ordinario f.r. di Diritto Internazionale, Università di Catania - già Componente ANAC
Guido Raimondi, già Presidente della Corte EDU - già Presidente di Sezione della Corte di Cassazione
Silvana Sciarra, Professore Emerito, Università di Firenze - Presidente Emerito della Corte Costituzionale
Giuseppe Tesaro, Professore f.r. di Diritto dell'UE, Università di Napoli "Federico II" - Presidente Emerito della Corte Costituzionale †
Antonio Tizzano, Professore Emerito, Università di Roma "La Sapienza" - Vice Presidente Emerito della Corte di giustizia dell'UE
Ennio Triggiani, Professore Emerito, Università di Bari †
Ugo Villani, Professore Emerito, Università di Bari

COMITATO EDITORIALE

Maria Caterina Baruffi, Ordinario di Diritto Internazionale, Università di Bergamo
Alfonso-Luis Calvo Caravaca, Catedrático Jubilado de Derecho Internacional Privado, Universidad Carlos III de Madrid
Ida Caracciolo, Ordinario di Diritto Internazionale, Università della Campania - Giudice dell'ITLOS
Pablo Antonio Fernández-Sánchez, Profesor Emérito de Derecho Internacional, Universidad de Sevilla
Inge Govaere, Director of the European Legal Studies Department, College of Europe, Bruges
Paola Mori, Ordinario f.r. di Diritto dell'Unione europea, Università "Magna Graecia" di Catanzaro
Lina Panella, Ordinario f.r. di Diritto Internazionale, Università di Messina
Lucia Serena Rossi, Ordinario di Diritto dell'UE, Università "Alma Mater Studiorum" di Bologna - già Giudice della Corte di giustizia dell'UE



COMITATO DEI REFEREES

Bruno Barel, Associato f.r. di Diritto dell'Unione europea, Università di Padova **Marco Benvenuti**, Ordinario di Istituzioni di Diritto pubblico, Università di Roma "La Sapienza"
Fiammetta Borgia, Ordinario di Diritto Internazionale, Università di Roma "Tor Vergata" **Francesco Buonomenna**, Associato di Diritto dell'Unione europea, Università di Salerno
Raffaele Cadin, Ordinario di Diritto Internazionale, Università di Roma "La Sapienza" **Ruggiero Cafari Panico**, Ordinario f.r. di Diritto dell'Unione europea, Università di Milano
Federico Casolari, Ordinario di Diritto dell'Unione europea, Università "Alma Mater Studiorum" di Bologna **Luisa Cassetti**, Ordinario di Istituzioni di Diritto Pubblico, Università di Perugia
Anna Cavaliere, Associato di Filosofia del diritto, Università di Salerno **Giovanni Cellamare**, Ordinario f.r. di Diritto Internazionale, Università di Bari
Giuseppe D'Angelo, Ordinario di Diritto e religione, Università di Salerno **Sara De Vido**, Ordinario di Diritto Internazionale, Università Ca' Foscari Venezia **Valeria Di Comite**, Ordinario di Diritto dell'Unione europea, Università di Bari "Aldo Moro" **Marcello Di Filippo**, Ordinario di Diritto Internazionale, Università di Pisa
Carmela Elefante, Associato di Diritto e religione, Università di Salerno **Rosario Espinosa Calabuig**, Catedrático de Derecho Internacional Privado, Universitat de València **Valentina Faggiani**, Professoressa Titular de Derecho Constitucional, Universidad de Granada
Caterina Fratea, Associato di Diritto dell'Unione europea, Università di Verona **Ana C. Gallego Hernández**, Profesora Ayudante de Derecho Internacional Público y Relaciones Internacionales, Universidad de Sevilla **Pietro Gargiulo**, Ordinario f.r. di Diritto Internazionale, Università di Teramo
Francesca Graziani, Associato di Diritto Internazionale, Università della Campania "Luigi Vanvitelli" **Giancarlo Guarino**, Ordinario f.r. di Diritto Internazionale, Università di Napoli "Federico II" **Elsbeth Guild**, Associate Senior Research Fellow, CEPS **Victor Luis Gutiérrez Castillo**, Profesor de Derecho Internacional Público, Universidad de Jaén **Ivan Ingravalle**, Ordinario di Diritto Internazionale, Università di Bari **Paola Ivaldi**, Ordinario di Diritto Internazionale, Università di Genova **Luigi Kalb**, Ordinario f.r. di Procedura Penale, Università di Salerno
Gianfranco Liace, Associato di Diritto dell'economia, Università di Salerno **Luisa Marin**, Ricercatore di Diritto dell'UE, Università dell'Insubria **Simone Marini**, Associato di Diritto dell'Unione europea, Università di Pisa **Fabrizio Marongiu Buonaiuti**, Ordinario di Diritto Internazionale, Università di Macerata **Rostane Medhi**, Professeur de Droit Public, Université d'Aix-Marseille **Michele Messina**, Ordinario di Diritto dell'Unione europea, Università di Messina-Esperto Giuridico presso la Rappresentanza Permanente d'Italia a Bruxelles
Stefano Montaldo, Associato di Diritto dell'Unione europea, Università di Torino **Violeta Moreno-Lax**, Senior Lecturer in Law, Queen Mary University of London
Claudia Morviducci, Professore Senior di Diritto dell'Unione europea, Università Roma Tre **Michele Nino**, Ordinario di Diritto Internazionale, Università di Salerno
Criseide Novi, Ordinario di Diritto dell'Unione europea, Università di Foggia **Anna Oriolo**, Associato di Diritto Internazionale, Università di Salerno **Leonardo Pasquali**, Ordinario di Diritto internazionale, Università di Pisa **Piero Pennetta**, Ordinario f.r. di Diritto Internazionale, Università di Salerno **Francesca Perrini**, Associato di Diritto Internazionale, Università di Messina
Gisella Pignataro, Associato di Diritto privato comparato, Università di Salerno **Emanuela Pistoia**, Ordinario di Diritto dell'Unione europea, Università di Teramo
Anna Pitrone, Associato di Diritto dell'Unione europea, Università di Messina **Concetta Maria Pontecorvo**, Ordinario di Diritto Internazionale, Università di Napoli "Federico II" **Pietro Pustorino**, Ordinario di Diritto Internazionale, Università LUISS di Roma **Santiago Ripol Carulla**, Catedrático de Derecho internacional público, Universitat Pompeu Fabra Barcelona
Angela Maria Romito, Associato di Diritto dell'Unione europea, Università di Bari **Gianpaolo Maria Ruotolo**, Ordinario di Diritto Internazionale, Università di Foggia
Teresa Russo, Associato di Diritto dell'Unione europea, Università di Salerno **Alessandra A. Souza Silveira**, Diretora do Centro de Estudos em Direito da UE, Universidade do Minho **Ángel Tinoco Pastrana**, Profesor de Derecho Procesal, Universidad de Sevilla
Sara Tonolo, Ordinario di Diritto Internazionale, Università degli Studi di Padova
Chiara Enrica Tuo, Ordinario di Diritto dell'Unione europea, Università di Genova **Talitha Vassalli di Dachenhausen**, Ordinario f.r. di Diritto Internazionale, Università di Napoli "Federico II" **Alessandra Viviani**, Ordinario di Diritto Internazionale, Università di Siena
Valentina Zambrano, Associato di Diritto Internazionale, Università di Roma "La Sapienza" **Alessandra Zanobetti**, Ordinario f.r. di Diritto Internazionale, Università "Alma Mater Studiorum" di Bologna

COMITATO DI REDAZIONE

Angela Festa, Docente incaricato di Diritto dell'Unione europea, Università della Campania "Luigi Vanvitelli"
Anna Iermano, Associato di Diritto Internazionale, Università di Salerno
Daniela Marrani, Associato di Diritto Internazionale, Università di Salerno
Rossana Palladino (Coordinatore), Associato di Diritto dell'Unione europea, Università di Salerno

Revisione linguistica degli abstracts a cura di

Francesco Campofreda, Dottore di ricerca in Diritto Internazionale, Università di Salerno





Indice-Sommario 2026, n. 2

Editoriale

La riforma della legislazione sulla cittadinanza tra Corte costituzionale e Corte di giustizia dell'Unione europea p. 1
Bruno Barel

Saggi, Articoli e Commenti

Free movement of persons in the agreement between the EU and the United Kingdom in respect of Gibraltar. Special status of military personnel p. 21
Pablo Antonio Fernández Sánchez

Storia diplomatica: Italia-Europa-Occidente p. 44
Massimo Panebianco

¿Hacia un modelo de Estado híbrido? Entre *court-packing* e intentos de revertir la *backsliding* p. 53
Valentina Faggiani

Vulnerabilità digitale del minore e forme di tutela nel contesto europeo p. 93
Gisella Pignataro

The case law of the European Court of Human Rights regarding contested territories: “Differentiated” jurisdiction as a panacea or as an Achilles’s heel? p. 120
Elisa Ruozzi

The EU legal framework on social security for migrants: A comparative assessment of national practices p. 139
Paolo Iafrate

Il danno ambientale sistemico e la soglia di gravità: tra qualificazione giuridica e tutela giurisdizionale p. 163
Adelaide Francesca Daniela Luminari



FOCUS

The EU as a Global Security Provider: Countering Transnational Crime and New Cooperation Architectures

Collected Papers of the Jean Monnet Module (2023-2026) Transnational Crime & EU Law: Towards Global Action against Cross-border Threats to Common Security, Rule of Law and Human Rights (EU-GLOBACT) – (Coordinator: Prof. Dr. Anna Oriolo)

Presentazione del Focus/Focus Overview
Anna Oriolo

p. 185

Parte I

Contrasto alla criminalità transnazionale e minacce globali/Countering Transnational Crime and Global Threats

Traffico illecito di armi via mare, criminalità transnazionale e sicurezza globale: verso un nuovo paradigma di legalità universale
Anna Oriolo

p. 191

The tragedy of the global commons in the age of artificial intelligence: Illegal mining, transnational crime, and the future of EU global enforcement
David Schultz

p. 216

The European legal framework on the return of cultural objects: An effective tool to foster civil and administrative cooperation between EU Member States?
Fulvia Staiano

p. 241

Il ruolo degli Stati nella prevenzione e nella repressione degli illeciti contro il patrimonio culturale subacqueo: obiettivi e strumenti comuni tra la Convenzione UNESCO del 2001 e le politiche dell'Unione europea
Patrizia Vigni

p. 257

Parte II

Nuove architetture di cooperazione e strumenti di contrasto dell'Unione europea/New Cooperation Architectures and Enforcement Tools of the European Union

Il principio di fiducia reciproca nella cooperazione giudiziaria penale a dieci anni dal caso *Aranyosi*. Alcune considerazioni sull'attualità del “doppio test” alla luce della sentenza *Commissione c. Ungheria (Valeurs de l'Union)*
Angela Festa

p. 281

Intelligence, diritti umani e sicurezza: criticità e prospettive in ambito internazionale ed europeo
Francesco Focillo

p. 312



War-crimes investigations: New technologies, new complexities, new vulnerabilities. A strategic shortfall or evolutionary opportunity for NATO p. 334
Luigi Bramati

AI tools for combating transnational crime within the EU p. 345
Roxana Matefi

Parte III

Responsabilità e giustizia penale/Accountability and Criminal Justice

Luci e ombre (soprattutto) occidentali sul consolidamento della giustizia penale internazionale p. 355
Paolo Bargiacchi

The EU's cross-border cybercrime enforcement and the limits of extraterritorial jurisdiction p. 388
Heybatollah Najandimanesh

La vittima di tratta al centro della sicurezza in Europa tra standard CEDU e nuove sfide nell'era digitale p. 410
Anna Iermano

La regolamentazione delle catene di approvvigionamento in Europa come strumento per combattere la criminalità: dall'opposizione alla convergenza dei modelli francese e italiano p. 442
Virginie Mercier

La responsabilità penale degli enti creditizi nella gestione delle misure restrittive UE: tra obblighi di garanzia e nuove fattispecie sovranazionali di incriminazione p. 453
Carmine Renzulli

Parte IV

Diritti umani e minacce transfrontaliere/Human Rights and Cross-Border Threats

La *transnational repression* quale minaccia “rinnovata” a diritti umani e sicurezza: la necessità di una risposta mirata da parte dell'Unione europea p. 465
Stefano Busillo

Children pornography, online sextorsion, revenge porn: the provisions of Greek penal code and the EU regulatory developments p. 507
Georgios Nouskalis

Intelligenza artificiale e “fenomeno religioso” nel prisma dei diritti umani p. 518
Daniela Marrani

Postfazione/Afterword p. 539
Angela Di Stasi

Appendice p. 541
EU-GLOBACT Policy Recommendations and Guidelines
Francesco Focillo, Emanuele Sorgente



VULNERABILITÀ DIGITALE DEL MINORE E FORME DI TUTELA NEL CONTESTO EUROPEO

Gisella Pignataro *

SOMMARIO: 1. Fragilità, vulnerabilità e ambiente digitale. – 2. Vulnerabilità digitale e minore età nel quadro giuridico europeo. – 3. Intensificazione dei pericoli nei sistemi di IA: le pratiche manipolative. – 4. La direzione europea di protezione e autonomia nei modelli inglese e francese. – 5. Forme di tutela privilegiata: prevenzione e rimedi tecnologici di verifica dell'età. – 6. Il regime sanzionatorio nel sistema integrato di tutele. – 7. Spazio digitale sicuro per i minori: il ruolo dell'asse educativo.

1. Fragilità, vulnerabilità e ambiente digitale

La giuridica rilevanza della fragilità della persona è stata a lungo circoscritta, a livello codicistico, entro le categorie generali della capacità di agire e della capacità di intendere e di volere, preordinate alla tutela da effetti pregiudizievoli di atti modificativi della propria sfera giuridica. Definiti con criteri normativi, per natura generali e astratti, tali concetti implicano la parificazione dei soggetti in possesso dei requisiti descritti e, per la minore età, la stridente equiparazione tra infanzia e adolescenza, graduata dalla capacità di discernimento nei rapporti di natura personale.

Con la codificazione dei contratti dei consumatori, la normativa di derivazione europea mette in crisi la presunzione di parità tra i contraenti capaci di agire e richiede agli Stati membri la protezione della debolezza del consumatore con strumenti variamente combinati, ma funzionali al riequilibrio delle inevitabili asimmetrie. Con un numero crescente di norme imperative vengono introdotti limiti incisivi all'autonomia contrattuale, tendenti a privilegiare la giustizia del contratto rispetto all'equivalenza soggettiva delle prestazioni, la formazione di una volontà consapevole con l'adempimento di specifici obblighi di informazione, perfino un controllo di tipo contenutistico. Si delinea così una condizione di debolezza trasversale ma equipollente, che prescinde dalle caratteristiche individuali fisiche, mentali, sociali o economiche

Double-blind peer reviewed article.

* Professore associato di Diritto privato comparato, Università degli Studi di Salerno. Indirizzo e-mail: gpignataro@unisa.it.

dell'interessato¹; gli strumenti di tutela sono di carattere generale e indifferenziato, correlati alla qualità di consumatore e all'efficienza causale dell'atto di consumo.

La personalizzazione delle forme di protezione e l'attenzione normativa per le fragilità del singolo individuo è acquisizione contemporanea, volta ad adattare le forme di tutela alle peculiarità di ciascun individuo e alle circostanze in cui opera (si pensi alla flessibilità dei contenuti di un provvedimento istitutivo dell'amministrazione di sostegno² o al divieto di pratiche commerciali scorrette qualificate con riferimento a una capacità cognitiva compromessa in ragione di condizioni personali, dovute all'età, a disabilità fisica o mentale o a una certa ingenuità³). Nell'ultimo decennio del XXI secolo, le nuove modalità di interazione tra i soggetti e l'intermediazione delle piattaforme hanno incrementato i fattori di vulnerabilità nello spazio digitale, ove si svolge un numero crescente di rapporti giuridici, e accentuato la fragilità e debolezza di tutti gli individui, laddove si conoscano *a priori* circostanze inerenti alla loro sfera personale in grado di orientarne il comportamento. La categoria dei soggetti vulnerabili, anch'essa trasversale, necessita di forme di protezione personalizzata, una costante nei documenti promossi da organismi internazionali e sovranazionali⁴, nell'auspicio di neutralizzare la debolezza decisionale di soggetti capaci, ma facilmente influenzabili, in presenza di fattori che condizionano la loro capacità di scelta e di autodeterminazione consapevole⁵.

Le vulnerabilità dell'ambiente digitale non identificano dunque una condizione giuridica definita, né sono correlate a uno *status* normativo, ma tendono ad attribuire rilevanza giuridica a fattori che possono ostacolare l'esercizio dei diritti⁶, effetto del carattere pervasivo delle nuove tecnologie ed espressione dell'incapacità di opporsi efficacemente alle insidie tipiche del sistema digitale, sia in termini di protezione dei dati personali che di autodeterminazione. Invero, l'esposizione in modo occulto al rischio di

¹ M.C. CHERUBINI, *Tutela del «contraente debole» nella formazione del consenso*, Torino, 2005, p. 3 ss. sulle tecniche idonee ad alterare il processo formativo della volontà di un soggetto capace.

² G. LISELLA, *La valorizzazione del carattere elastico dell'amministrazione di sostegno in funzione di una piena promozione e protezione della persona fragile*, in *Famiglia*, 2022, n. 4, p. 455 ss.; ID., *Elasticità dell'amministrazione di sostegno: limiti*, *ivi*, 2022, n. 5, p. 625 ss.; M. GIROLAMI, *Dalla crisi dell'amministratore di sostegno al mandato di protezione*, in *Rivista di diritto civile*, 2021, n. 5, p. 858 ss.

³ Art. 5, par. 3, direttiva 2005/29/CE, 11maggio 2005 relativa alle pratiche commerciali sleali tra imprese e 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»).

⁴ Sviluppano un concetto meno formalistico della capacità la Convenzione dell'Aja sulla protezione internazionale degli adulti (2000), la Convenzione delle Nazioni Unite sui diritti delle persone con disabilità (2006), le Raccomandazioni del Consiglio d'Europa (2009 e 2014), ma il concetto è richiamato anche dalla giurisprudenza della Corte europea dei diritti dell'uomo e formalizzato nell'AI Act (2024).

⁵ Una tutela adeguata richiede pertanto l'adattamento alle fragilità dell'individuo e dunque alle caratteristiche del caso: S. PATTI, *Il contraente «fragile»*, in *Rivista trimestrale di diritto e procedura civile*, 2025, n. 2, p. 232; A. SARTOR, *Persona fragile e contratto giusto*, Padova, 2023, *passim*.

⁶ A. GENTILI, *La vulnerabilità sociale. Un modello teorico per il trattamento legale*, in *Rivista critica del diritto privato*, 2019, p. 46, per il quale la vulnerabilità non è astratta, ma è specifica, per cui non può introdurre una figura teorica del diritto; F. LUNA, *Identifying and Evaluating Layers of Vulnerability - A Way Forward*, in *Developing World Bioethics*, 2019, n. 19, p. 86 ss., descrive a livello pratico differenti gradazioni di vulnerabilità, non necessariamente stabili né attribuibili a categorie di individui o a gruppi specifici. Differenti stati di vulnerabilità, anche di natura transitoria, possono coesistere in un determinato contesto e richiedono una tutela giuridica di intensità crescente, a seconda del livello di vulnerabilità.

compressione della libertà di scelta rende ciascun individuo potenzialmente vulnerabile, se chiamato a operare in un ambiente virtuale che non domina, ma di cui si avvale per acquisire beni e servizi digitali⁷. Siffatta asimmetria digitale, in aggiunta a condizioni di debolezza strutturali, introduce una variabile incrementale che amplifica le possibilità di sfruttamento dell'inesperienza e l'esposizione a pratiche manipolatorie idonee a erodere l'autonomia e a condizionare le scelte dell'utente come consumatore, contraente o persona in termini di *privacy* e di dignità⁸. Debolezza non marginale nei rapporti già squilibrati sul piano informativo, anche in virtù della raccolta massiva di dati personali e dell'utilizzo di sistemi di IA, ma anche nei rapporti tra pari⁹, dove l'abuso delle fragilità può essere agevolato dal ricorso a servizi di intermediazione *on line*¹⁰ e avere, nella minore età, l'effetto dirompente di condizionare anche lo sviluppo della personalità.

In questo contesto la novità più interessante del diritto contrattuale europeo, i c.d. *pre-contractual information duties*, imposti dal legislatore europeo in quanto strumento idoneo a esaltare l'effettiva autonomia contrattuale basata sulla trasparenza¹¹, viene ridimensionata dal rischio di personalizzazione dell'informativa, strumentale all'interesse del gestore del sistema. Per evitare l'effetto paradossale che l'adempimento diventi causa di quella debolezza che si intendeva correggere con la norma imperativa¹², il quadro normativo adottato dal legislatore europeo nell'adattamento del mercato unico all'evoluzione digitale vieta il condizionamento della volontà dell'utente e lo sfruttamento delle vulnerabilità sia nell'architettura grafica delle piattaforme (*Digital*

⁷ E. BATTELLI, *Vulnerabilità della persona e debolezza del contraente*, in *Rivista di diritto civile*, 2022, n. 5, p. 939 ss.

⁸ R. MONTINARO, *Online platforms: new vulnerabilities to be addressed in the European legal framework. Platform to consumer relations*, in *European Journal of Privacy Law & Technologies*, 2020, n. 2, p. 62.

⁹ Condizionamenti sono frequenti nei rapporti per natura asimmetrici tra professionista e consumatore, tra titolare del trattamento dei dati e il soggetto cui i dati si riferiscono, tra produttore e utente dove il ricorso a tecniche di profilazione algoritmica o di personalizzazione degli annunci commerciali o dei prezzi consentono di creare vulnerabilità e dunque pregiudizi, anche con effetti sistemici se il Considerando n. 69 del *Digital Service Act* avverte «Quando ai destinatari del servizio vengono presentate inserzioni pubblicitarie basate su tecniche di targeting ottimizzate per soddisfare i loro interessi e potenzialmente attirare le loro vulnerabilità, ciò può avere effetti negativi particolarmente gravi. In alcuni casi, le tecniche di manipolazione possono avere un impatto negativo su interi gruppi e amplificare i danni per la società, ad esempio contribuendo a campagne di disinformazione o discriminando determinati gruppi. Le piattaforme online sono ambienti particolarmente sensibili per tali pratiche e presentano un rischio per la società più elevato. Di conseguenza, i fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione, come definite all'articolo 4, punto 4), del regolamento (UE) 2016/679, utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, dello stesso regolamento, anche utilizzando categorie di profilazione basate su tali categorie speciali».

¹⁰ M. INFANTINO, C. CREA, *Digital Vulnerability as a Tool for Social Justice in European Private Law*, in transformativeprivatelaw.com/digital-vulnerability-as-a-tool-for-social-justice-in-european-private-law/

¹¹ S. PATTI, *Autonomia contrattuale e diritto privato europeo*, in *Contratto e impresa*, 2003, n. 3, p. 633 ss.

¹² N. HELBERGER, M. SAX, J. STRYCHARZ e H.W. MICKLITZ, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, in *Journal of Consumer Policy*, 2022, vol. 45, p. 187.

Service Act)¹³, sia nel funzionamento dei sistemi di IA (art. 5 *AI Act*)¹⁴. Ma se l'intento è di consentire alle parti di operare nel mercato in condizioni di parità sostanziale e di rafforzare la fiducia nel suo leale funzionamento, il divieto con il suo contenuto negativo è condizione necessaria ma non sufficiente a neutralizzare vulnerabilità già rilevate; diversamente se viene integrato con un obbligo positivo di protezione.

A tale tipologia è riconducibile l'obbligo di rimozione delle condizioni di fragilità, che impediscono all'utente di autodeterminarsi liberamente quando si relaziona con un potere privato che gestisce l'ambiente e il rapporto giuridico, inserito nel sistema di tutela preventiva privilegiato dal legislatore europeo. La rete e i sistemi di IA mettono a disposizione potenti strumenti per pratiche di manipolazione e sfruttamento contrari ai valori europei; adottare misure specifiche di assistenza nella formazione del consenso o di prevenzione di condizionamenti o discriminazioni ad opera di terzi potrebbe rientrare nell'obbligo di cura e di salvaguardia dell'utente riconducibile al contenuto precettivo della clausola di buona fede adattata alla dinamicità dell'ambiente digitale¹⁵. La stessa *data protection by design e by default*, richiamata dal *General Data Protection Regulation* (GDPR), configura una tutela preventiva e dinamica che obbliga il responsabile del trattamento dati ad adottare misure protettive variabili in ragione dei possibili pregiudizi, della specificità del settore in cui si opera e delle costanti innovazioni tecnologiche, in conformità ai valori europei di rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza e non discriminazione.

Analoga varietà di contenuti presenta la vulnerabilità applicata alla minore età: pur aggettivando la condizione - il minore è vulnerabile per definizione - l'idiosincrasia con ogni forma di automatismo mette in crisi la tradizionale equivalenza tra protezione e divieto, non riproponibile nell'ambiente digitale per il contributo dell'interazione in rete alla formazione dell'identità individuale, come rimarcato dal legislatore europeo.

2. Vulnerabilità digitale e minore età nel quadro giuridico europeo

La polivalenza della rete e degli strumenti tecnologici, che in essa si sviluppano, apre orizzonti illimitati alle capacità individuali nello svolgere una pluralità di funzioni, supportare servizi diversificati, potenziare l'apprendimento, i diritti di espressione e di

¹³ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), in GU L 277 del 27.10.2022, pp. 1-102.

¹⁴ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, 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), in GU L, 2024/1689, 12.7.2024.

¹⁵ A. BERNES, *Persona vulnerabile, ambiente digitale e obblighi di protezione*, in *Il diritto di famiglia e delle persone*, 2025, n. 1, p. 180 ss.; A. NICOLUSSI, *Responsabilità da contatto sociale qualificato*, in C. SCOGNAMIGLIO (dir.), *Enciclopedia del diritto, I tematici, Responsabilità civile*, Milano, 2024, p. 1076 ss.; J. BALKIN, *Free Speech is a Triangle*, in *Columbia LawReview*, 2018, p. 2053 ss.

partecipazione; ma le medesime potenzialità implicano anche esposizione a rischi dei soggetti più fragili. Nel timore di questi ultimi, il diritto ha riservato ai minori un impianto normativo protezionistico con l'incapacità di agire, che riduce il potere decisionale oltre *les actes de la vie quotidienne*, in palese contrasto con la condizione di nativi digitali per la sua rigidità. Invero, dalla generazione di fine XX secolo¹⁶ i minori ben conoscono le dinamiche della rete, hanno dimestichezza con i *digital devices* e l'accesso a tali strumenti è sempre più precoce; taluni applicativi risultano altresì utili allo sviluppo dell'identità personale, *in fieri* per definizione: l'incremento dei canali di accesso a informazioni e conoscenze, la personalizzazione dei processi di apprendimento, l'intrattenimento con attività di gioco educativo ne valorizzano la crescita e la capacità di evoluzione, che richiede il riconoscimento di un'autonomia progressiva nel contesto digitale¹⁷.

La constatazione non impedisce di continuare a includere l'età evolutiva tra le forme paradigmatiche di vulnerabilità intrinseca. Anzi, gli orizzonti indefiniti della rete espongono a una serie di rischi che, seppur non esclusivi dello *status* minorile, necessitano di maggiori cautele se influenzano la formazione ed educazione dei minori. La progettazione manipolativa dell'interfaccia grafica della piattaforma (con cui portare l'utente a compiere azioni non desiderate o a eseguire procedure talmente complesse da scoraggiare il controllo effettivo sui dati personali), la limitata alfabetizzazione, contenuti inappropriati o pericolosi possono amplificare gli effetti nocivi nell'ambiente virtuale. L'Organizzazione per la cooperazione e lo sviluppo economico (OECD) nel 2021¹⁸ ha catalogato le minacce per i minori, classificate in quattro macrocategorie legate ai contenuti¹⁹, alla condotta²⁰, ai contatti²¹, o quali consumatori²², cui si aggiungono ulteriori

¹⁶ Il riferimento è alla c.d. Generazione Z.

¹⁷ A. LA SPINA, *L'identità del minore nella realtà on-life tra protezione e autodeterminazione*, in *Famiglia e diritto*, 2024, n. 10, p. 921.

¹⁸ Il Rapporto "*Children in the digital environment: Revised typology of risks*", poi ripreso dalla Comunicazione alla Commissione europea "*Approval of the content of a draft Communication from the Commission - Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065*", Brussels, 14.7.2025, C/2025/4764 final.

¹⁹ Potenzialmente dannosi per i minori sono i contenuti che incitano all'odio – illegali – e la disinformazione, mentre promuovere l'autolesionismo, il suicidio, i disturbi alimentari o la violenza estrema sono contenuti dannosi in sé, in quanto producono gravi conseguenze negative sulla salute mentale e sul benessere fisico dei minori.

²⁰ Il riferimento è ai comportamenti che i minori potrebbero adottare attivamente *on line* e che possono rappresentare un rischio per sé stessi e per gli altri, quando pubblicano o inviano contenuti e messaggi d'odio, contenuti violenti, pornografici o illegali, come materiale pedopornografico o contenuti terroristici, ovvero se induttivi di comportamenti problematici, quale la partecipazione a sfide pericolose o il sexting (invio o condivisione di testi, foto, audio o video a contenuto sessualmente esplicito).

²¹ Trattasi di situazioni in cui i minori sono vittime delle interazioni, in contrapposizione all'autore, tramite incontri motivati dall'odio, programmati con l'intenzione di danneggiare il minore, illegali e penalmente perseguibili. Si pensi all'adescamento *on line*, alla coercizione ed estorsione sessuale *on line*, all'abuso sessuale tramite webcam, cyberbullismo e tratta di esseri umani a scopo di sfruttamento sessuale oppure, sul piano economico, a pratiche di frode *on line* come *phishing*, frodi sui *marketplace* e furto di identità.

²² L'economia digitale espone i minori a rischio di *marketing*, di profilazione commerciale, di danni finanziari con frodi o spese di ingenti somme di denaro senza la conoscenza o il consenso del rappresentante legale, per la sicurezza o acquisto e consumo di droghe, medicinali, alcol e altri prodotti illegali o pericolosi.

rischi a carattere trasversale²³. In questo contesto si inserisce il quadro normativo europeo del mercato digitale, rappresentato dal GDPR, dal *Digital Services Act* (DSA) e dall'*Artificial Intelligence Act* (AI Act), che colloca la protezione del minore in uno schema di governance basata sul rischio elevato, per come incide sui diritti fondamentali, ma non cristallizzata.

Nella società dell'informazione, proiettata alla digitalizzazione crescente del mondo analogico, l'accesso alla rete contribuisce al processo di formazione verso una graduale ma consapevole capacità di autodeterminazione, che un generico divieto per motivazioni protettive inevitabilmente ostacolerebbe. Nella visione paidocentrica della famiglia, l'accesso diventa un diritto e concorre all'armonico sviluppo della persona; in questi termini impegna la responsabilità genitoriale quale componente del dovere di cura in tutti gli ambiti di competenza e, in mancanza di un adeguato supporto familiare o educativo, le istituzioni, specie se tratti personali o esperienze di vita rendono alcuni bambini più esposti al danno²⁴. Il problema è garantirne l'effettività, ovvero il corretto esercizio. A tal fine sicuramente l'identità del figlio rappresenta il criterio-guida, l'ascolto aiuta nella selezione degli interessi e il controllo rientra nei doveri educativi in rapporto dialettico, anche fisiologicamente conflittuale, con i genitori. Ma non è semplice confrontarsi con strumenti da decodificare e in continua evoluzione, oltretutto con un'interferenza parentale inversamente proporzionale alla maturità del figlio, nel periodo dell'infanzia come nell'adolescenza, in un costante bilanciamento tra protezione e autonomia.

Rafforza l'elemento dell'autonomia il legislatore europeo quando, nella categoria unitaria della minore età, ha introdotto una diversificazione tra minori e adolescenti, allorché riconosce, per questi ultimi, la liceità del trattamento dei dati personali se il minore che presta il consenso autonomamente abbia più di sedici anni, riconoscendo però agli Stati membri la facoltà di fissare una diversa soglia di età, purché non inferiore a

²³ Trattasi di rischi che influiscono gravemente sul benessere dei minori, considerati altamente problematici, legati alle tecnologie avanzate e ai nuovi pericoli effetto dell'evoluzione della tecnologia, come i chatbot basati sull'intelligenza artificiale che potrebbero fornire informazioni dannose o essere utilizzati per l'adescamento, sfruttando le vulnerabilità, o l'uso di tecnologie biometriche per possibili abusi, furti di identità; ai rischi per la salute e il benessere fisico (obesità o anoressia), mentale, emotivo. L'uso eccessivo di piattaforme *on line* possono avere effetti negativi sulla salute e il benessere fisico e mentale dei minori, come dipendenza, depressione, disturbi d'ansia, disturbi del sonno e isolamento sociale. Rischi ulteriori possono riguardare la *privacy* e la protezione dei dati grazie all'accesso alle informazioni sui minori e alla geolocalizzazione, che semplifica la possibilità di avvicinare i minori; la sicurezza dei minori, sia fisica che informatica; derivanti in generale dall'uso improprio della piattaforma *on line* o delle sue funzionalità.

²⁴ N. PATTI, V. PUNZO, R. ROMANO, *Child vulnerabilities in the digital environment: comparative insights and operational guidelines*, in *Opinio Juris in Comparatione*, 2025, n. 2, p. 110 s. Le autrici parlano di vulnerabilità disposizionali, che rendono alcuni individui più fragili di altri, come nella condizione di minore adottato che spesso comporta fragilità emotive e relazionali o legate all'identità, intensificate o talvolta strumentalizzate nei contesti digitali.

tredici anni²⁵. Una scelta che si inserisce nel solco tracciato dai documenti internazionali²⁶ sulla valorizzazione del carattere dinamico della formazione dell'identità personale e il riconoscimento al minore di una autonomia graduale a seconda della capacità di discernimento, prima della capacità di agire²⁷, seppur ancorata al criterio formale dell'età, meno variabile della capacità di discernimento. È significativa, perché introduce una sorta di maggiore età digitale per la disposizione dei dati che, in Italia, è fissata a 14 anni, a meno che il consenso non abbia altra base giuridica²⁸, mentre il consenso va prestato e il trattamento va autorizzato dal titolare della responsabilità genitoriale per il minore di età inferiore²⁹; è più rigorosa, ma non antitetica rispetto alla più liberale normativa statunitense, che fissa a tredici anni l'età minima per accedere ai servizi della società dell'informazione³⁰.

²⁵ Art. 8, GDPR: «Per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni».

²⁶ Convenzione di New York sui diritti del fanciullo, del 20 novembre 1989, ratificata in Italia con legge 27 maggio 1991, n. 176; negli altri Stati membri dell'Unione europea la ratifica è intervenuta sempre nel corso degli anni '90 dello scorso secolo, mentre gli Stati Uniti non hanno ancora provveduto a ratificarla. Nel Commento generale n. 25 (2021) il Comitato delle Nazioni Unite sui diritti dell'infanzia ha approfondito l'applicazione del principio che riconosce anche ai minori la titolarità di diritti autonomi, dignità e capacità di agire negli ambienti digitali. L'auspicio è un approccio normativo che rispetti le capacità in evoluzione dei bambini, adotti misure di protezione adeguate all'età, promuova l'alfabetizzazione digitale di chi si prende cura di loro, imponga obblighi rigorosi ai fornitori di servizi digitali a garanzia di elevati standard di trasparenza, *privacy* e sicurezza. All'imperativo di proteggere, ineliminabile, occorre dunque affiancare il compito di responsabilizzare i minori per abituarli ad essere soggetti attivi nel corso delle loro esperienze digitali.

²⁷ P. STANZIONE, *I contratti del minore*, in *Europa e diritto privato*, 2014, n. 4, p. 1237 ss.; R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2021, p. 18 ss.

²⁸ Il problema investe la capacità di stipulare negozi *on line*: benché la maggiore età digitale del quattordicenne sia limitata al consenso al trattamento dei dati, non è ipotizzabile una netta scissione rispetto alla capacità negoziale se l'accesso alle piattaforme implica la sottoscrizione delle clausole di accesso, che sono clausole contrattuali, che possono prevedere la vendita dei dati personali o condizioni inique: M.G. STANZIONE, *Consenso al trattamento di dati personali nella dimensione europea*, in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2024, p. 97 ss.

²⁹ Art. 2-quinquies, co. 1, del novellato Codice Privacy, introdotto dal D.Lgs. 101/2018: «In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale». La norma è in linea con la l. 71/2017, la disciplina sul cyberbullismo, che consente al minore ultraquattordicenne di rivolgersi in nome e per conto proprio al gestore del sito internet, ove siano stati pubblicati dati personali pregiudizievoli, per ottenere la rimozione dei contenuti lesivi; alla medesima età il minore può rivolgersi anche al Garante per la protezione dei dati personali in caso di inerzia o se il titolare del trattamento non è identificabile.

³⁰ Il *Children's Online Privacy Protection Act* del 1998 (COPPA) è una legge federale degli Stati Uniti, emanata il 21 ottobre 1998, 15 U.S.C. §§ 6501-6506. L'intento iniziale era di fissare la soglia d'età a 16 anni, limite contrastato sia dalle grandi società di e-commerce portatrici di interessi privati in quanto non volevano rinunciare a una redditizia fetta di mercato che non avrebbe potuto beneficiare di beni e servizi della società dell'informazione, sia dai gruppi per le libertà civili per non escludere molti ragazzi dall'accesso ad Internet e dunque a una serie di informazioni. Discutibile è la discussione sugli interessi terzi, senza partire dagli studi sullo sviluppo cognitivo e sulla capacità di esprimere un consenso informato o di comprendere o elaborare i contenuti cui hanno accesso.

La rilevanza giuridica del diverso livello di maturità digitale potrebbe esonerare i genitori dal dovere di sorveglianza o scoraggiarli, in quanto alimenta la conflittualità generazionale se i figli si sentono legittimati ad opporsi alla loro guida o supervisione, avvertita come illecita intromissione genitoriale. Potere-dovere che invece le regole codicistiche sulla capacità riconoscono come necessario e non delegabile, seppur da modulare in ragione della reale maturità e capacità di discernimento, pur sempre nel rispetto del diritto alla riservatezza. Peraltro, ricca è la letteratura sull'inidoneità del consenso ad apprestare un'adeguata tutela, per la sua discutibile capacità di assicurare una reale autodeterminazione, l'opacità dei processi di raccolta, elaborazione e trattamento dei dati, la superficiale o carente lettura dell'informativa talvolta difficile da decifrare, nonché per il condizionamento di un consenso necessario per accedere al servizio³¹.

L'approccio protezionistico spicca invece nella più recente regolamentazione europea dove, nel predisporre misure adeguate a tutelare i diritti, considera la vulnerabilità intrinseca alla minore età unitariamente intesa. Nel DSA come nell'*AI Act* la disciplina identifica nel minore la potenziale vittima sia quale fruitore dei servizi delle piattaforme *online*, sia quale utente dei sistemi di IA. L'esposizione al rischio giustifica l'introduzione di divieti che hanno come destinatari la categoria dei fornitori, rappresentanti, distributori dei sistemi³². L'obiettivo è sottrarre il minore a indebite influenze e condizionamenti, anche se la tutela complessiva resta frammentata.

All'esigenza di sicurezza e protezione si ispira il DSA e l'adozione di regole che rispondono al solo bisogno di tutela rispetto al rischio di esposizione dei minori a contenuti che potrebbero essere nocivi per la salute e lo sviluppo fisico, mentale e morale³³. A tal fine la Commissione ha elencato le raccomandazioni principali rivolte ai

³¹ E. TOSI, *Intelligenze artificiali e dati personali tra AI Act e GDPR: prime riflessioni su vulnerabilità digitale e crepuscolo del consenso*, in *Il diritto dell'informazione e dell'informatica*, 2025, nn. 4-5, p. 726 ss.; ID., *La tutela risarcitoria della persona nel contesto delle asimmetrie digitali*, *ivi*, 2025, n. 1, p. 49; ID., *Circolazione contrattuale dei dati personali tra GDPR e nuovo Codice del Consumo*, *ivi*, 2023, n. 2, p. 198 ss.; ID., *Dati personali e contratto: un ossimoro apparente*, in *European Journal of Privacy Law & Technologies*, 2023, n. 2, 79 ss.; S. ORLANDO, *Consenso al trattamento e liceità*, in *Persona e mercato*, 2024, p. 333 ss.; ID., *Per un sindacato di liceità del consenso*, *ivi*, 2022, p. 527 ss.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Il diritto dell'informazione e dell'informatica*, 2018, p. 689 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del Diritto*, 2017, p. 363 ss.

³² L'art. 9, par. 9 dell'*AI Act*, espressione dell'approccio basato sul rischio, obbliga i fornitori a prestare attenzione all'eventualità che il sistema di IA ad alto rischio possa avere un impatto negativo sui minori o su altri soggetti particolarmente vulnerabili. Analogamente, l'art. 28 del *Data Service Act*, dedicato alla protezione *on line* dei minori, impone ai fornitori di piattaforme accessibili ai minori di adottare misure adeguate e proporzionate al fine di garantire un elevato livello di tutela della vita privata, della sicurezza e della protezione dei minori e di rispettare il divieto di profilazione di questi ultimi; inoltre, l'art. 14, comma 3, DSA, da leggere in combinato disposto con il Considerando n. 46 dello stesso Regolamento, sancisce che se un servizio di intermediazione è principalmente destinato a minori o utilizzato prevalentemente da questi, il prestatore di tale servizio deve spiegare, in modo a loro comprensibile, le relative condizioni e restrizioni.

³³ Si leggano i Considerando 71, 81 e 89 DSA, nonché gli artt. 28, 34, par. 1, lett. b) e d); e 35, par. 1, lett. j).

fornitori delle piattaforme *on line* per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione³⁴. Analogamente, per la limitata capacità di valutare in modo critico la realtà e i rischi sottesi alle interazioni tramite sistemi di IA, l'*AI Act*³⁵ dedica particolare attenzione alla sicurezza dei minori, più esposti alla creazione di legami con applicazioni che favoriscono la manipolazione o comportamenti assimilabili alla dipendenza. Una condizione comune all'infanzia e all'adolescenza, inserita tra le pratiche vietate dall'art. 5 del Regolamento. I bambini interagiscono con le tecnologie di IA tramite giochi interattivi che spingono il minore a superare sfide sempre più rischiose, perfino abusando della loro curiosità e del desiderio di gratificazione³⁶; giochi che analizzano il comportamento e le preferenze, potendo così proporre ricompense personalizzate; programmi che generano dipendenza, e dunque un uso eccessivo e compulsivo del gioco³⁷. Ma anche gli adolescenti possono essere manipolati dagli algoritmi, che suggeriscono video da guardare, musica da ascoltare, chi frequentare senza che il minore sia in grado di valutare in modo critico la *ratio* dell'interazione. Gli effetti di tali dipendenze possono protrarsi anche in età adulta, come problemi di salute fisica per mancanza di esercizio fisico, di sonno, deterioramento della vista, o di concentrazione e riduzione delle abilità cognitive, causa di scarsi risultati scolastici o difficoltà di relazione.

Una delle espressioni di tale difficoltà è la relazione con amici virtuali, che simulano relazioni anche affettive e spingono i minori alla condivisione di dati personali oltre a

³⁴ Numerose sono le Raccomandazioni oggetto dell'*Approval of the content of a draft Communication from the Commission - Guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065*, cit.: impostare gli account dei minori in privato per impostazione predefinita in modo che le loro informazioni personali, i dati e i contenuti dei social media siano nascosti a quelli con cui non sono collegati; modificare i sistemi di raccomandazione delle piattaforme per ridurre il rischio che i bambini incontrino contenuti dannosi; consentire ai bambini di bloccare e disattivare qualsiasi utente e garantire che non possano essere aggiunti ai gruppi senza il loro esplicito consenso; proibire agli account di scaricare o scattare schermate di contenuti pubblicati da minori per impedire la distribuzione indesiderata di contenuti sessualizzati o intimi e l'estorsione sessuale; disabilitare per impostazione predefinita le funzionalità che contribuiscono a un uso eccessivo; garantire che la mancanza di alfabetizzazione commerciale dei bambini non sia sfruttata e che non siano esposti a pratiche commerciali che possono essere manipolative, portare a spese indesiderate o comportamenti di dipendenza; introdurre misure per migliorare gli strumenti di moderazione e comunicazione, che richiedono un feedback tempestivo, e requisiti minimi per gli strumenti di controllo parentale.

³⁵ Considerando n. 48 *AI Act*, secondo cui «i minori godono di diritti specifici sanciti dall'articolo 24 della Carta e dalla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, ulteriormente sviluppati nell'osservazione generale n. 25 della Convenzione delle Nazioni Unite dell'infanzia e dell'adolescenza per quanto riguarda l'ambiente digitale, che prevedono la necessità di tenere conto delle loro vulnerabilità e di fornire la protezione e l'assistenza necessarie al loro benessere. È altresì opportuno tenere in considerazione, nel valutare la gravità del danno che un sistema di IA può provocare, anche in relazione alla salute e alla sicurezza delle persone, il diritto fondamentale a un livello elevato di protezione dell'ambiente sancito dalla Carta e attuato nelle politiche dell'Unione». Si consideri anche la nuova strategia europea per un'internet migliore per i ragazzi (BIK+) (COM(2022) 212 final).

³⁶ Il bambino potrebbe essere incoraggiato ad arrampicarsi sui mobili, a esplorare scaffali posizionati in alto, a manipolare oggetti taglienti in cambio di ricompense digitali o elogi virtuali.

³⁷ I giochi possono essere programmati per creare dipendenza, sfruttando vulnerabilità tipiche dei minori, come la limitata capacità di comprendere le conseguenze a lungo termine, la mancanza di autocontrollo, il desiderio di gratificazione istantanea.

condizionarne i comportamenti. Come vedremo nel caso Replika³⁸, il Garante ha arginato in Italia il rischio di trattamento incontrollato dei dati, ordinandone la cessazione fino a quando non fossero adottate misure idonee ad evitarlo.

Obiettivo europeo è sicuramente garantire sicurezza e protezione ai minori, ma senza rinunciare al riconoscimento di una maggiore autonomia e responsabilità nell'ambiente digitale, secondo quanto espresso nella Dichiarazione comune sui diritti e principi digitali, proclamata congiuntamente da Parlamento europeo, Consiglio e Commissione³⁹. Una duplice esigenza che spetta alle legislazioni nazionali contemperare.

3. Intensificazione dei pericoli nei sistemi di IA: le pratiche manipolative

La manipolazione nell'interazione dei minori con l'intelligenza artificiale, specie generativa, rientra non soltanto nel generale divieto di pratiche a rischio inaccettabile, ma ha rappresentato una delle prime scadenze vincolanti per fornitori e utilizzatori di sistemi di IA, seguita dall'attivazione del relativo sistema sanzionatorio. I contenuti del divieto sono specificati dalle Linee guida pubblicate dalla Commissione europea ad integrazione dell'art. 5 dell'*AI Act*⁴⁰, considerata l'incidenza degli strumenti digitali nello sviluppo dell'identità personale. Evidenti sono i rischi rispetto a capacità e competenze cognitive inevitabilmente *in fieri*, specie se l'applicazione di IA è rivolta direttamente ai minori, generalmente non educati e preparati in maniera adeguata a esserne utenti, ma la duplice valenza dello strumento digitale induce ad astenersi da astratte generalizzazioni.

Tutto il sistema dell'IoT (*Internet of Things*) rientra in questa categoria e interessa trasversalmente i minori, dall'infanzia all'adolescenza. Progettato per registrare, trattare,

³⁸ GPD, provvedimento del 2 febbraio 2023 [9852214], n. 39.

³⁹ Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, in *GUCE*, 23 gennaio 2023, C23/1. L'obiettivo è di promuovere un modello europeo di trasformazione digitale, che metta al centro le persone, rispetti i valori europei e i diritti fondamentali dell'UE, riaffermi i diritti umani universali a beneficio delle persone, delle imprese e della società. Nel Capitolo V, dedicato a "Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità" si legge testualmente: «Protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale. 20. I bambini e i giovani dovrebbero essere messi nelle condizioni di compiere scelte sicure e informate e di esprimere la propria creatività nell'ambiente digitale. 21. Si dovrebbero migliorare le esperienze, il benessere e la partecipazione all'ambiente digitale dei bambini e dei giovani attraverso materiali e servizi adeguati all'età. 22. Occorre prestare particolare attenzione al diritto dei bambini e dei giovani di essere protetti da tutti i reati commessi attraverso le tecnologie digitali o facilitati da tali tecnologie. Ci impegniamo a: a) offrire a tutti i bambini e i giovani opportunità per acquisire le necessarie capacità e competenze, tra cui l'alfabetizzazione mediatica e il pensiero critico, per navigare e interagire nell'ambiente digitale in modo attivo e sicuro e per compiere scelte informate; b) promuovere esperienze positive per i bambini e i giovani in un ambiente digitale sicuro e adeguato all'età; c) proteggere tutti i bambini e i giovani dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi online e impedire che lo spazio digitale sia utilizzato per commettere o facilitare reati; d) proteggere tutti i bambini e i giovani dal tracciamento, dalla profilazione e dal targeting illegali, in particolare a fini commerciali; e) coinvolgere i bambini e i giovani nell'elaborazione delle politiche digitali che li riguardano».

⁴⁰ Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA), Bruxelles, 29.7.2025, C (2025) 5052 final, nel rispetto della prima scadenza del 2 febbraio 2025 per il divieto di pratiche a rischio inaccettabile gravante su fornitori e utilizzatori di sistemi di IA e del 2 agosto 2025 per l'attivazione del sistema sanzionatorio.

conservare, e trasferire dati grazie al collegamento in rete, essendo associati a identificativi univoci, realizzano una connessione tra mondo fisico e ambiente digitale, senza che l'utente ne sia pienamente consapevole, specie se l'uso è contestuale allo svolgimento di altre attività. *Smart TV*, *smart watch*, *wearable devices* garantiscono, infatti, la continua accessibilità alle informazioni secondo la logica *multitasking*, al pari degli *smart toys*, giocattoli capaci di interagire con le persone e con l'ambiente circostante tramite microfoni, sensori, fotocamere, geolocalizzazione, nonché di dialogare con altri dispositivi connessi in rete. Al problema del trasferimento dei dati e rischio di utilizzo oscuro e imprevedibile degli stessi, si aggiunge la capacità dell'oggetto di interpretare i dati raccolti se integrato con l'IA, di interagire con l'utente adattandosi ai contesti, di personalizzare le decisioni a seconda dell'interlocutore⁴¹. Un sistema di IA applicato ai giochi, capace di osservare e registrare le abitudini, i comportamenti, le voci del minore, crea empatia e affidamento utile alla manipolazione e non soltanto per finalità di *marketing* commerciale⁴². L'interazione con prodotti umanizzati riduce le difese e induce il minore-utente a condividere informazioni non soltanto in difetto di consapevolezza, ma in violazione dei principi fondamentali sul trattamento dei dati personali, la disciplina del consenso e la minimizzazione⁴³.

Altra forma di condizionamento occulto della libertà di scelta e di pensiero deriva dagli algoritmi creati per adattare i contenuti alle preferenze dell'utente tramite la profilazione di interessi espressi in precedenza o comuni alla categoria di utenti, adulti o minori⁴⁴. Si ritrovano nel suggerimento di video, nello *shopping* in rete, nei servizi di ristorazione, nelle proposte di viaggio, nella stessa informazione. La proposizione di determinati contenuti in sequenza può creare effetti pregiudizievoli di dipendenza, in particolare per i minori, su cui la piattaforma riesce a monetizzare grazie alla diretta connessione tra gli introiti della raccolta pubblicitaria e le visualizzazioni e interazioni degli utenti. Uno stop a tale prassi quale pratica commerciale scorretta è stato imposto dall'AGCOM alla piattaforma e all'app TikTok in occasione della diffusione di una *challenge* idonea a minacciare la sicurezza psico-fisica dei minori in particolare⁴⁵.

⁴¹ J. ZHANG, D. TAO, *Empowering Things with Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things*, in *IEEE IoT-J*, 8(10), 2021, p. 7789 ss.

⁴² 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*, Baden-Baden, 2024, p. 446. Genesis Toys, come my friend Cayla, una bambola destinata a bambine della fascia di età tra i cinque e i dieci anni, pubblicizzata per la sua capacità di capire e rispondere in tempo reale quasi su tutto, o robot intelligenti con cui instaurare conversazioni in tempo reale, sono prodotti che svolgono funzioni tipicamente umane, compresa la capacità di provare sensazioni e stati d'animo o inclinazioni.

⁴³ S. RIGAZIO, *L'empowerment del minore nella dimensione digitale*, Modena, 2024, p. 40 ss.

⁴⁴ Laddove i social network tendono a mostrare agli utenti contenuti in linea con loro precedenti interazioni, si creano le c.d. *filter bubbles*, dove i giovani rischiano di ricevere informazioni unilaterali e progressivamente sempre più estreme: G. ZICCARDI, *I minori nella società digitale tra verifica dell'età, deepfake e disinformazione. Alcune considerazioni informatico-giuridiche*, in *Sociologia del diritto*, 2025, n. 2, p. 143 ss. sugli effetti nella formazione dell'identità dei ragazzi che, se privi di strumenti critici, possono sviluppare percezioni falsate della realtà e aderire a ideologie estreme.

⁴⁵ AGCM, provv. 14 marzo 2024, n. 31124, caso "PS12543 – TikTok cicatrice francese, dove si rilevava che «l'esigenza di effettuare un controllo stringente sui contenuti di TikTok discende dai meccanismi cognitivi dei ragazzi e adolescenti, e dall'importanza per i giovani di appartenere ad un gruppo tramite l'adozione

L'effetto lesivo della pratica è ancora più ampio se si considera l'induzione incrementale alla permanenza sulla piattaforma in virtù dell'automatismo della selezione dei contenuti personalizzati per ciascun utente tramite un sistema di raccomandazione basato sulla profilazione algoritmica⁴⁶, non mitigato dall'opzione per un sistema di selezione alternativo – pur predisposto – per difetto di informazioni chiare e l'opzione per il meccanismo di scelta c.d. *opt-out*.

Effetti analoghi possono produrre i *chatbot*, programmi informatici basati sul linguaggio, che dialogano con gli esseri umani e per questo riscuotono successo tra i minori. Per la loro capacità di ingenerare nell'interlocutore fiducia, tali strumenti possono influenzare la crescita e lo sviluppo del minore e produrre effetti lesivi se linguaggio, toni e contenuti non siano appropriati in relazione alla fascia di età, alla capacità di discernimento, al grado di formazione o al contesto sociale ed economico di provenienza. L'app Replika, facilmente scaricabile sullo smartphone e progettata per offrire un amico virtuale con cui interagire per dialogare, ascoltare, dare consigli, confortare, esprimere emozioni, calmare l'ansia aiutare la socializzazione e la ricerca dell'amore, è risultata pericolosa per i soggetti ancora in fase di sviluppo o in stato di fragilità emotiva. Come avvenuto in passato con la piattaforma TikTok⁴⁷, il Garante italiano per il trattamento dei dati personali è dovuto intervenire prima disponendo la limitazione provvisoria dell'attività di trattamento dei dati personali per mancato rispetto del principio di trasparenza e insufficienti garanzie a tutela dei minori per i contenuti spesso invadenti, inopportuni se non volgari⁴⁸, per poi dichiarare illecito il trattamento dei dati per

di comportamenti emulativi di "leader", anche virtuali. L'adolescente ha una capacità limitata di valutare le conseguenze delle proprie azioni; la capacità di discernimento, infatti, si acquisisce a livello neurologico solo nell'età adulta, considerato che il sistema nervoso raggiunge l'apice del proprio sviluppo intorno all'età di 30 anni. I ragazzi presentano poi maggiori difficoltà degli adulti nel distinguere la realtà dalle suggestioni della finzione; stante l'assenza di strumenti di inibizione generazionale, i giovani tendono a prendere decisioni più avventate degli adulti, dettate anche dal loro senso di onnipotenza».

⁴⁶ AGCM, provv. 14 marzo 2024, n. 31124, cit: «Il potenziale lesivo per i minori e i soggetti vulnerabili deriva non solo dalla proposizione di singoli video pericolosi ad un ampio numero di utenti, ma è amplificato dalla riproposizione, ad opera del sistema di raccomandazione, di video analoghi in successione a ciascun singolo utente. Nonostante il sistema di raccomandazione personalizzato sia presentato all'utente come un fattore positivo che contribuisce alla scoperta del mondo, "che ispira la creatività e porta gioia", TikTok è consapevole che la raccomandazione in sequenza di determinati contenuti può creare effetti pregiudizievoli, in particolare per i minori e soggetti vulnerabili. Appare infatti prevalere, anche nei confronti di tali categorie di utenti, l'interesse di TikTok a generare un importante effetto di addiction che essa riesce a monetizzare». Il 6 febbraio 2026 Bruxelles ha pubblicato conclusioni preliminari nel procedimento formale avviato per presunta violazione del *Digital Services Act*, sostenendo che alcune scelte di interfaccia e raccomandazione possono generare comportamenti compulsivi e compromettere il benessere psicofisico degli utenti, soprattutto dei minori. La combinazione di scroll infinito, *autoplay*, notifiche *push* e raccomandazione altamente personalizzata sembra ridurre la capacità di autodeterminazione, favorendo un uso definito "*autopilot mode*". L'auspicio è l'adozione di un *Digital Fairness Act*.

⁴⁷ GPDP, provv. 22 gennaio 2021, con cui si dispose il blocco dell'uso della piattaforma per tutti gli italiani per i quali non fosse stata verificata con certezza l'età anagrafica a protezione dei minori, misura adottata a seguito del decesso a Palermo di una bambina di 10 anni mentre partecipava a una pericolosa *challenge* diffusa su TikTok. In tale occasione fu evidenziata la corresponsabilità familiare e la necessità di una vigilanza attiva: il Garante può bloccare il social, ma il primo controllore è il genitore.

⁴⁸ GPDP, provv. 2 febbraio 2023, n. 9852214, caso Replika.

violazione del principio di liceità e di trasparenza e obbligare la società titolare a conformare il sistema di verifica dell'età⁴⁹.

Il tema non è più la tutela della riservatezza del minore, ma della sua persona⁵⁰. Il limite di questi sistemi è rappresentato infatti dall'effetto manipolativo, funzionale a interessi estranei alle finalità dichiarate. Invero, non può escludersi a priori la loro utilità se utilizzati con finalità formative: gli *smart toys* permettono percorsi di apprendimento diversificati e personalizzati, con materiali adattati alle esigenze del singolo utente, e di monitorare i progressi e la crescita; i *chatbot* possono essere utilmente impiegati nei contesti scolastici, per favorire l'apprendimento o la maggiore accessibilità per gli studenti con dislessia o con disabilità fisiche. La soluzione educativa non può dunque essere il divieto, ma la responsabilizzazione di tutti gli attori.

Nei confronti degli operatori del mercato il legislatore europeo opta per un approccio normativo centralizzato nel predeterminare i rischi associati all'uso dell'intelligenza artificiale, imporre regole stringenti e la previa valutazione dell'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment*) in base al livello di pericolosità del sistema, suggerire di uniformarsi spontaneamente o su provvedimento delle Autorità indipendenti, disciplinare le sanzioni pecuniarie. Ma la tutela effettiva dei minori non può prescindere da una supervisione attenta e costante del titolare della responsabilità genitoriale, legittimando provvedimenti giurisdizionali limitativi o ablativi nelle situazioni più gravi⁵¹, nella consapevolezza che i compiti educativi di indirizzo esigibili dipendono da numerosi fattori, come l'età, la capacità di autodeterminazione,

⁴⁹ GPD, provv. 10 aprile 2025, n. 10130115, caso Replika: neppure dopo il blocco iniziale la società ha saputo porre rimedio alle carenze denunciate, causa della sanzione con una multa di 5 milioni di euro.

⁵⁰ Nel 2021 un'inchiesta giornalistica del Wall Street Journal, svolta in collaborazione con una ex dipendente di Meta, Frances Haugen, ha pubblicato i c.d. Facebook files per dimostrare come i gestori fossero perfettamente a conoscenza degli effetti dannosi di Instagram sulla salute mentale di bambini e adolescenti. Il *Surgeon General of the United States*, il capo esecutivo dello *United States Public Health Service Commissioned Corps* e portavoce delle questioni di salute pubblica all'interno del governo federale, ha iniziato a pubblicare una serie di *advisory* per richiamare l'attenzione sulla crisi nazionale della salute mentale, del benessere dei giovani, sulle profonde conseguenze sulla salute derivanti dalla c.d. *social disconnection*. Dagli studi scientifici già allora emergeva una correlazione allarmante tra utilizzo dei social da parte di minori e l'aumento delle malattie legate alla salute mentale come depressione, ansia, disturbi alimentari, disturbi dell'attenzione e della qualità del sonno. Prima che la Commissione europea aprisse il procedimento contro Meta, oltre 40 Stati americani e il Distretto di Columbia hanno citato in giudizio il colosso, accusando meta di aver ingannato i consumatori in merito agli effetti dannosi sui più giovani oltre ad aver commercializzato i suoi prodotti ai minori di 13 anni, contravvenendo la legge federale. Poiché la normativa applica le sanzioni soltanto laddove il gestore della piattaforma ne sia effettivamente a conoscenza, se il minore si registra mentendo sulla propria età, il fornitore di servizi potrebbe non essere soggetto a sanzioni. Il provvedimento della Corte suprema di Los Angeles, 25 marzo 2026, di condanna al pagamento di 3 milioni di dollari a titolo di risarcimento rappresenta in importante precedente.

⁵¹ Trib. Minorenne Milano, ord. 22 aprile 2025 n. 828, in *One Legale*, ha disposto la nomina di un curatore speciale e il provvedimento ex art. 330 c.c. di presa in carico da parte dei servizi sociali e dell'Unità operativa di Neuropsichiatria dell'Infanzia e dell'Adolescenza competente per territorio, nel caso di un minore che aveva interrotto di sua iniziativa il percorso scolastico obbligatorio e versava in una situazione di totale isolamento per dipendenza da *device*. L'intervento si era reso necessario per l'evidente rischio evolutivo e comportamenti violenti nei confronti della madre, costretta a denunciarlo e a rivolgersi ai servizi sociali. Non si è pervenuto a provvedimenti ablativi della responsabilità genitoriale in ragione la condotta collaborativa della madre, ma l'allontanamento dal contesto familiare anche allargato rispondeva a carenze del ruolo educativo e di cura morale.

l'alfabetizzazione digitale del minore e dei membri della famiglia, il livello di educazione, lo *status* socio-economico, il sostegno delle istituzioni scolastiche, la collocazione geografica.

Al difetto di alfabetizzazione è ascrivibile l'eccessiva esposizione *online* del minore indotta dai genitori, in ossequio alla discutibile abitudine di rendere pubblico il privato⁵², talvolta strumentale all'aumento del valore commerciale del proprio profilo se trattasi di *influencer*. Invero, se i figli sono adolescenti, capaci di esprimere un valido consenso, la pubblicazione senza la loro espressa approvazione deve considerarsi sempre illecita; né la liceità è necessariamente intrinseca alla titolarità della responsabilità genitoriale rispetto ai ragazzi di età inferiore. Il fenomeno ha assunto rilevanza giuridica nell'ambito del contenzioso tra *ex partner* per la pubblicazione *on line* di immagini e altre informazioni sui figli senza il consenso dell'altro genitore, tema tendenzialmente risolto dai tribunali con pronunce, spesso cautelari, che ordinano la rimozione del materiale e ne inibiscono il nuovo inserimento in difetto di accordo genitoriale⁵³. Condotta invero censurabile principalmente per abuso dell'immagine o dei dati altrui, più che per carenza di formale autorizzazione: a parte i rischi di sicurezza dei dati personali, la loro diffusione in rete può incidere negativamente sulla personalità dei minori, che potrebbero non riconoscersi in una identità digitale creata da altri⁵⁴. Le informazioni e le immagini condivise *on line* circolano in modo imprevedibile e incontrollabile, ben potendo entrare nella disponibilità di un numero imprecisato di persone nell'ambito di un circuito interconnesso. Complice la memoria della Rete, che non dimentica⁵⁵ ma può al massimo de-indicizzare le informazioni⁵⁶, l'identità digitale circolata è difficilmente modificabile in futuro e potrebbe incidere sensibilmente sul progressivo processo di autodeterminazione del minore e sulla libera costruzione della sua personalità. Danno che non può essere scongiurato dal consenso di entrambi i genitori, non rientrando tale potere nella responsabilità genitoriale, in quanto la condivisione è funzionale all'interesse del

⁵² Si parla del fenomeno del c.d. *sharenting*, neologismo elaborato con la crasi dei termini *sharing* e *parent*.

⁵³ Cass., 21 agosto 2024, n. 23018, in *Giust. civ. Mass.*, 2024, che cassa la pronuncia di rigetto dell'istanza di risarcimento per abuso dell'immagine di minori, l'illecita diffusione del ritratto del bambino per fini di pubblicità commerciale, effettuata senza il consenso di uno dei genitori, senza aver preventivamente accertato una seria ed effettiva lesione alla riservatezza dell'immagine della persona, bene primario tutelato in sé che può essere pregiudicato a prescindere dall'indicazione del nome o delle generalità del minore. Trib. Rieti, 17 ottobre 2022, n. 443, in *D & G*, 21 novembre 2022, per la pubblicazione sul social network Facebook di alcune fotografie dei bambini, da parte della sorella della madre, in assenza del previo consenso dell'uomo; Trib. Rieti, 7 marzo 2019, in *IUS Famiglie*, 16 luglio 2019, sulla pubblicazione da parte della compagna del padre di immagini ritraenti i minori, in assenza del consenso espresso da entrambi i genitori esercenti la responsabilità genitoriale; Tribunale Mantova, 19 settembre 2017, in *Dejure.it*, circa l'inserimento da parte della madre di numerose foto dei figli sui social network, anche dopo l'intervenuto accordo fra i genitori a carattere inibitorio.

⁵⁴ Trib. Roma, 23 dicembre 2017, in *Dejure.it*, sulla richiesta del minore di iscrizione in un College negli USA, nonostante il rischio di interruzione delle normali relazioni sociali legate all'età, per il timore di essere considerato diverso da parte dei coetanei a conoscenza delle questioni personali del minore per le notizie diffuse dalla madre sui social network.

⁵⁵ G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Diritto dell'informazione e dell'informatica*, 2010, n. 3, p. 391 ss.

⁵⁶ Corte Giustizia, Grande Sezione, 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*.

genitore e non del figlio, in contrasto con il dovere di protezione, che comprende diritti non meramente dichiarativi, come il rispetto dell'immagine e della riservatezza⁵⁷. La responsabilità genitoriale non conferisce un potere assoluto e discrezionale sul minore, ma incontra limiti strutturali nel riconoscimento della dignità e di spazi di autonomia.

L'ambiente digitale amplifica altresì i doveri di controllo dei genitori sull'interazione in rete dei minori, esposti alla responsabilità per danni a terzi ai sensi dell'art. 2048 o dell'art. 2047 c.c., ove il figlio non sia capace di intendere e di volere: trattasi di responsabilità aggravata per fatto altrui a titolo di colpa presunta per omissione dei doveri parentali, a garanzia patrimoniale del danneggiato. Si parla di responsabilità oggettiva per rischio tipico o da *status*, in quanto per l'esonero non è sufficiente la prova negativa di non aver potuto impedire il fatto, ma è richiesta la prova positiva di avere debitamente assolto al compito educativo, di avere effettivamente controllato che l'educazione sia stata assimilata e di aver esercitato una vigilanza adeguata all'età, indole e ambiente⁵⁸. Interpretazione che finisce per scaricare sui soli genitori la responsabilità, senza coinvolgere gli attori economici, in un contesto che si sottrae a schemi predefiniti di tutela. La materiale impossibilità di vigilanza e l'autonomia dei minori capaci nello spazio digitale, che preclude anche al genitore attento di seguire i figli in rete, implica un onere probatorio arduo, impossibile da assolvere e antitetico all'impostazione di questa come responsabilità per fatto proprio, difficoltà riconosciuta da giurisprudenza minoritaria⁵⁹. Il rigore interpretativo che parifica l'operato dei minori in rete non è infatti conciliabile con la capacità digitale del minore ultraquattordicenne e il rispetto del suo diritto alla riservatezza⁶⁰; diversamente per i figli di età inferiore, rispetto ai quali è esigibile un controllo preventivo dei rischi e l'attivazione degli strumenti che la tecnologia mette a disposizione. *De iure condendo*, soltanto una progettazione dei servizi digitali incentrata sulla tipologia di destinatario potrà segnare un mutamento di strategia nel garantire una

⁵⁷ Discutibile è nella giurisprudenza l'esclusione della responsabilità quando le pubblicazioni avvengono su social network chiusi. La loro configurazione privata non garantisce il controllo dei contenuti, che possono essere replicati, scaricati e fatti circolare: V. BARBA, *Derecho a la identidad digital y protección de niños, niñas y adolescentes frente a la exposición prematura en redes*, in *Revista de Ciencias Sociales*, n. 87, Universidad de Valparaíso, 2025.

⁵⁸ Cass., 28 marzo 2001, n. 4481, in *Danno e responsabilità*, 2001, p. 498 ss., con nota critica di V. CARBONE, *Non rispondono i genitori per gli incidenti causati dal minore in motorino*, e in *Famiglia*, 2001, p. 1171 ss., con commento favorevole di S.L. PATTI, *Responsabilità dei genitori: una sentenza in linea con l'evoluzione europea*; Corte App. Campobasso, 25 agosto 2025, n. 254, in *Dejure.it*: «La responsabilità dei genitori ex art. 2048 c.c. non è attenuata dalla precoce emancipazione dei minori frutto del costume sociale, avendo essi l'onere di impartire ai figli l'educazione necessaria per non recare danni a terzi nella loro vita di relazione, dovendo rispondere delle carenze educative a cui l'illecito commesso dal figlio sia riconducibile»; analogamente Cass., 18 ottobre 2024, n. 27061, *ivi*; Trib. Cassino 18 settembre 2018, *ivi*; Corte App. Lecce 9 aprile 2018, n. 393, in *Guida dir.*, 2018, p. 31; Trib. Minorenni Caltanissetta, 8 ottobre 2019, in *www.ilFamiliarista.it*, 20 marzo 2020, con nota di S. MOLFINO, *I genitori devono controllare i figli minorenni nell'utilizzo dello strumento tecnologico. Anche se ultraquattordicenni?*; Trib. Minorenni Caltanissetta, 16 luglio 2018, *ivi*, 20 marzo 2019.

⁵⁹ Trib. Cagliari, 21 giugno 2001, in *Riv. giur. sarda*, 2002, p. 407, che consente di superare la presunzione *iuris tantum* di aver impartito al minore un'educazione e un'istruzione consona alle proprie condizioni familiari e sociali; Trib. Verona il 18 febbraio 2000, in *Giurisprudenza italiana*, 2000, p. 1407.

⁶⁰ F. SCIA, *Minori e illeciti digitali nel sistema della responsabilità civile*, in *Nuova giur. civ. comm.*, 2001, f. 3, p. 573 ss.

efficace tutela preventiva volta a guidare e non ostacolare i minori nella fruizione di tutte le opportunità disponibili nel contesto digitale, utili allo sviluppo di una personalità in formazione. Prospettiva cui tendono le legislazioni nazionali, per come hanno iniziato a recepire le indicazioni europee.

4. La direzione europea di protezione e autonomia nei modelli inglese e francese

Alla sintesi tra responsabilità e protezione si ispira l'*Age-Appropriate Design Code* (AADC, denominato anche *Children's Code*)⁶¹, redatto dall'*Information Commissioner's Office* (ICO)⁶², un primo tentativo di disciplina del rapporto tra minori e ambiente digitale adottato dall'Autorità indipendente inglese responsabile del trattamento dei dati ed entrato in vigore nel 2020, con cui si individuano quindici standard di progettazione rivolti ai fornitori di servizi *on line* accessibili dai minorenni. Il quadro normativo, incentrato sui minori, è integrato da misure di sicurezza *on line*, oggetto dell'*Online Safety Act*, entrato in vigore nel 2023⁶³, anch'esso informato all'equilibrio tra tutela dei minori, libertà di espressione e diritto alla *privacy* nel rispetto dei principi di proporzionalità e necessità. Gli standard minimi del *Children's Code*, informati al preminente interesse del minore, riassumono le principali regole quali la priorità dei suoi diritti rispetto agli interessi commerciali, adattamento dei servizi alle differenti fasce d'età o adozione del medesimo elevato livello di protezione per tutti gli utenti, disattivazione delle impostazioni predefinite per la geolocalizzazione e attivazione di livelli di *privacy* superiori, divieto di tecniche manipolative o persuasive, come i *dark pattern*, che incoraggiano la condivisione dei dati e di qualsiasi trattamento dannoso per il benessere fisico, mentale o emotivo del minore. Ad essi si aggiunge il richiamo al rigoroso rispetto delle regole del GDPR quali la trasparenza, la minimizzazione dei dati, la limitazione della profilazione e la semplificazione degli strumenti per l'esercizio dei propri diritti digitali.

Nell'*Online Safety Act* gli intermediari digitali sono tenuti alla valutazione e mitigazione del rischio, con particolare attenzione ai contenuti accessibili dai minori; l'autorità di regolamentazione gode di ampi poteri di vigilanza e di coazione nell'applicazione della legge. La sicurezza implica, per i fornitori dei servizi, l'obbligo di valutare i rischi associati a contenuti, funzionalità e interazioni digitali suscettibili di

⁶¹ Il testo, denominato anche *Children's Code*, è pubblicato al seguente indirizzo web:

<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/>.

⁶² Il regolamento è stato pubblicato il 27 gennaio 2020 ed è entrato in vigore il 2 settembre 2020, vincolante ai sensi del *Data Protection Act*. Si applica a qualsiasi prodotto o servizio connesso a Internet che possa essere utilizzato da una persona di età inferiore ai 18 anni, da progettare nei *best interests* dei minori e della loro salute, sicurezza e *privacy*. A tal fine, vanno garantite di *default* le impostazioni di *privacy* più restrittive, e dunque che siano raccolti di prassi soltanto i dati strettamente necessari per fornire gli elementi del servizio, da non divulgare a terzi; inoltre, le politiche e i controlli sulla *privacy* occorre che siano presentati in modo chiaro e accessibile loro, incluso il divieto di *dark patterns*.

⁶³ UK Parliament, *Online Safety Act*, 2023, in <https://www.legislation.gov.uk/ukpga/2023/50>.

influenzare i minori, cui si deve uniformare la progettazione di algoritmi e interfacce utente volte a minimizzare i potenziali danni. A tal fine è fondamentale l'implementazione di sistemi affidabili di verifica o stima dell'età per selezionare i contenuti e impedire ai minori l'accesso a quelli dannosi, per garantirne l'equilibrio e una serena crescita. A supporto si inseriscono requisiti rigorosi in materia di trasparenza e di responsabilità delle piattaforme.

Obiettivo dichiarato è la proiezione del sistema di protezione verso una cultura digitale diffusa, che coinvolga, accanto ai bambini, tutti gli adulti che, nei diversi ruoli, interagiscano con loro, in qualità di genitori, educatori, assistenti sociali, volontari, amministratori o funzionari pubblici, secondo una strategia trasversale di alfabetizzazione digitale rispettosa dei bambini.

Il tema delle modalità di relazione dei minori con l'ambiente digitale e l'opportunità di una riforma sistemica è in discussione anche nel sistema francese, affrontato a livello programmatico nel rapporto *Enfants et Écrans. À la Recherche du Temps Perdu*, redatto da una Commissione di esperti⁶⁴. Premessa l'analisi di contesto circa la reale esposizione dei minori e l'impatto delle tecnologie sulla loro salute fisica e mentale⁶⁵, il rapporto valuta l'efficacia e le criticità della normativa vigente per suggerire le possibili strategie di intervento e progettare un ambiente sicuro. L'intento è di integrare la normativa vigente, frammentaria e settoriale, e rafforzare la coerenza di sistema: alla logica limitativa in tema di gioco d'azzardo⁶⁶ o nell'incitamento all'odio online⁶⁷, propositiva con l'istallazione di *default* di sistemi di *parental control*⁶⁸ e di salvaguardia contro le pratiche subliminali degli influencer⁶⁹, si oppone un modello per arginare preventivamente i rischi e liberare il potenziale educativo e partecipativo delle nuove

⁶⁴ Il testo del rapporto, pubblicato nell'aprile 2024, è reperibile all'indirizzo <https://www.elysee.fr/admin/upload/default/0001/16/fbec6abe9d9cc1bff3043d87b9f7951e62779b09.pdf>.

⁶⁵ Per un'analisi di rischi e degli effetti sul benessere fisico e mentale, si rinvia a G. PIGNATARO, *Pratiche manipolative e persone deboli: quali tutele nell'era della IA*, in V. D'ANTONIO, B. MEOLI (a cura di), *Responsabilità civile per i danni da intelligenza artificiale*, Santarcangelo di Romagna (RN), 2026, p. 349 ss.

⁶⁶ Loi n. 2010-476 du 12 mai 2010 *relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne*, reperibile all'indirizzo <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000022204510>.

⁶⁷ Loi n. 2023-566 du 7 juillet 2023 *visant à instaurer une majorité numérique et à lutter contre la haine en ligne*, reperibile all'indirizzo <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>, mai entrata in vigore. La legge aveva indicato in quindici anni la "maggiore età digitale" per l'accesso alle piattaforme dei social media; i successivi dubbi di compatibilità con il diritto dell'Unione europea hanno indotto il legislatore a emanare una legge sulla *privacy* e sui diritti d'immagine dei minori, la Loi n. 2024-120 du février 2024 *visant à garantir le respect du droit à l'image des enfants*, reperibile all'indirizzo [⁶⁸ Loi n. 2022-300 du 2 mars 2022 *visant à renforcer le contrôle parental sur les moyens d'accès à internet*, reperibile all'indirizzo <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045287677>.](https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049163317/2025-04-16/#:~:text=LOI%20n%202024%2D120,des%20enfants%20(1)%20%2D%20Légifrance.Sulla efficacia delle norme francesi sui diritti di immagine dei minori, M. SAULIER, <i>Garantir le respect du droit à l'image des enfants: un objectif ambitieux, une efficacité douteuse?</i>, in <i>Actualité juridique Famille</i>, 2024, n. 3, p. 116 ss.</p>
</div>
<div data-bbox=)

⁶⁹ Loi n. 2023-451 du 9 juin 2023, *visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*, reperibile all'indirizzo <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047663185>.

tecnologie tramite regole di comportamento imposte agli operatori economici, soluzione preferita rispetto all'idea del controllo esterno.

Per liberare la navigazione in rete da ambienti stereotipati e commercializzati e proteggere la libertà di scelta, essenziale alla formazione dell'identità, il rapporto indica una serie di aree di intervento, dirette rispettivamente a identificare e vietare pratiche manipolative, consentire l'accesso graduale in base all'età nell'uso di schermi e tecnologie digitali, alfabetizzazione digitale per un'educazione mirata a preparare i giovani all'autonomia e alla responsabilità in rete, estendere la formazione ai genitori e a tutti gli adulti che lavorano con i bambini per aiutarli a comprendere il ruolo delle tecnologie digitali, implementare un quadro di governance per definire le strategie di concreto intervento.

In questa ottica, indicato l'obiettivo nella progettazione delle piattaforme e vietate le pratiche dannose, grava sui fornitori di servizi digitali l'onere della prova sull'impatto dei loro algoritmi; alla libertà dai condizionamenti è preordinata una sorta di diritto alla configurazione, per garantire agli utenti, e ai minori in particolare, la possibilità di modificare consapevolmente le impostazioni predefinite che li riguardano. Fondamentale è l'introduzione di efficaci meccanismi di verifica dell'età per un approccio graduale e programmato ai dispositivi⁷⁰, oltre a maggiori investimenti in contenuti educativi per una cittadinanza digitale consapevole. I pilastri delle prospettive di riforma convergono dunque sulla progettazione etica delle piattaforme e dei sistemi di IA, sul rafforzamento dell'autonomia dei minori e sul ruolo educativo affidato a genitori e operatori con l'auspicio della loro alfabetizzazione digitale.

L'approccio antropocentrico della regolamentazione europea si traduce, a livello di legislazione nazionale, nel riequilibrio delle vulnerabilità non improntato alla mera logica protettiva, ma al temperamento della necessaria tutela con una responsabilizzazione dinamica, che tenga conto dell'evoluzione delle capacità del minore, concetti non antitetici ma complementari e inversamente proporzionali. Obiettivo non realizzabile senza la cooperazione tra sviluppatori, fornitori di servizi e autorità di regolamentazione. L'*AI Act* impone obblighi vincolanti a operatori e utilizzatori dei sistemi di intelligenza artificiale ad alto rischio, richiedendo trasparenza, valutazione del rischio, documentazione e monitoraggio continuo. Ma il governo etico della tecnologia passa per la collaborazione e non contrapposizione tra tutti gli attori, comprese le famiglie. Programmi di formazione accessibili in rete e disponibilità di risorse informative potrebbero assistere i genitori, per aiutarli a non identificare la protezione con i divieti, ma con la promozione dell'autonomia e del pensiero critico dei figli.

⁷⁰ Il programma suggerito vieta l'esposizione agli schermi in età inferiore ai sei anni, introduzione di telefoni cellulari e dispositivi digitali personali con funzioni limitate e senza connessione a internet dagli undici anni, connessione internet dai 13 anni, ma con restrizioni sui social media e sui contenuti illegali fino a consentire l'accesso ai social media all'età di quindici anni.

5. Forme di tutela privilegiata: prevenzione e rimedi tecnologici di verifica dell'età

Un primo passo per la costruzione di un ambiente digitale sicuro dipende dal ricorso generale a seri sistemi di verifica dell'età: sollecitati a livello normativo europeo e nazionale, iniziano a operare a seguito degli interventi delle Autorità garanti. Il trattamento massiccio dei dati con sistemi automatici non è di regola compatibile con i principi di equità, trasparenza, necessità, proporzionalità, minimizzazione; a maggior ragione impedisce la personalizzazione della protezione per gruppi di utenti vulnerabili. Protezione che, per i minori, assume la duplice funzione di bilanciamento della tipica fragilità endemica e di contributo allo sviluppo armonico della persona. Si comprende pertanto la centralità di un sistema affidabile di verifica dell'età mentre, in difetto, ogni tecnica di prevenzione è destinata al fallimento.

Utili indicazioni sulle tendenze regolamentari si possono desumere dalla recente delibera AGCOM nei confronti di gestori di siti web e piattaforme di condivisione che diffondono in Italia immagini e video di carattere pornografico⁷¹, tenuti ad adottare le modalità tecniche per l'accertamento della maggiore età dell'utente a prescindere dalla sede di stabilimento in altro Stato membro⁷². I sistemi di verifica sono riconducibili a due tipologie: la scansione di un documento identificatore rigido, tipo carta di identità, patente di guida o passaporto, oppure l'identificazione tramite un fornitore terzo, che può avvalersi di altre fonti di informazione (carte di credito, registri elettorali, servizi bancari o assicurativi). L'Autorità esclude la conformità alla *privacy* dei sistemi che si basano sulla raccolta diretta di documenti di identità, sulla stima dell'età desunta dalla cronologia di navigazione e sul trattamento di dati biometrici (riconoscimento facciale dal confronto

⁷¹ Delibera AGCOM, 8 aprile 2025, n. 96/25/CONS, relativa all'Adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge 13 novembre 2023, n. 159 (c.d. decreto Caivano). Le modalità tecniche suggerite sono indicate nell'Allegato A alla delibera AGCOM, 8 aprile 2025, *loc. cit.*, relativo alle “*Modalità tecniche e di processo per l'accertamento della maggiore età degli utenti ai fini dell'accesso a determinati servizi forniti dai gestori di siti web e dalle piattaforme di condivisione di video che diffondono in Italia immagini e video a carattere pornografico, ai sensi dell'articolo 13 bis del decreto-legge 5 settembre 2023, n. 123 convertito con modificazioni dalla legge 13 novembre 2023, n. 159*”.

⁷² Le metodologie di verifica dell'età in uso sono elencate nell'allegato B alla delibera AGCOM, 8 aprile 2025, *loc. cit.*, che descrive il Quadro europeo sulle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti di seguito elencate: (i) Autodichiarazione: gli utenti dichiarano la propria età/fascia di età senza fornire altre prove. (ii) Identificatori rigidi: gli utenti forniscono documenti di identità verificati (ad esempio passaporto) per dimostrare la loro età. (iii) Carte di credito: utilizzo dei dati della carta di credito per verificare che un utente abbia più di 18 anni. (iv) Identità basata su blockchain: utilizzo di tecnologie decentralizzate come blockchain per creare identità digitali degli utenti, per utilizzare tali identità per l'*age verification*. (v) Conferma del titolare del conto: basarsi sulla conferma di un titolare di conto verificato esistente che un altro utente ha l'età richiesta per utilizzare la piattaforma. (vi) Autenticazione multiplatforma: utilizzo di account utente già esistenti con piattaforme di grandi dimensioni (ad esempio Google, Apple ecc.) per autenticare l'età di un utente per altri prodotti/servizi. (vii) Stima del viso: utilizzo dell'intelligenza artificiale per analizzare le caratteristiche del viso di una persona per stimarne l'età. (viii) Profilazione comportamentale: utilizzo dell'intelligenza artificiale per analizzare l'attività online degli utenti per stimarne l'età. (ix) Test di capacità: testare la capacità o l'attitudine dell'utente per stimare l'età. (x) Servizi di assicurazione sull'età di terze parti: utilizzo di società terze per i servizi di assicurazione sull'età. Le terze parti potrebbero utilizzare uno qualsiasi degli altri metodi per la garanzia dell'età.

con una fotografia riportata su un documento di identità o un *selfie*), filtro rivelatosi inadeguato per la possibilità di aggiramento del meccanismo e utile a proteggere soltanto gli operatori a discapito degli esercenti la responsabilità genitoriale.

La preferenza è orientata verso gli *Identity Provider* certificati, soggetti terzi giuridicamente e tecnicamente indipendenti rispetto ai fornitori dei contenuti *on line* (una banca, un operatore telefonico, un ente pubblico o un soggetto privato che ha già identificato altrimenti l'utente), selezionati sulla base di requisiti soggettivi e oggettivi indicati dalla normativa di settore, soggetti alla vigilanza dell'Agenzia per l'Italia Digitale (AGID), secondo il modello del doppio anonimato a garanzia di maggiore riservatezza⁷³. La certificazione ha una funzione giuridica, non soltanto tecnica: obbliga i fornitori all'adozione di standard documentati e conformi ai principi di trasparenza e proporzionalità, soggetti a verifica periodica. Sul piano procedurale necessita di una serie di passaggi logicamente distinti: richiesta del sito o piattaforma di verificare l'età e invio di un elemento neutro (file o stringa alfanumerica), privo di riferimenti al servizio cui si vuole accedere; l'utente richiede al soggetto terzo liberamente scelto di certificare l'età da provare, generando un nuovo elemento di prova, senza specificare l'utilizzo che ne vorrà fare⁷⁴; invio della prova al sito o alla piattaforma cui spetta il controllo di validità e coerenza con quanto richiesto, senza venire a conoscenza dell'identità dell'utente⁷⁵. Per semplificare, l'*Identity Provider* può mettere a disposizione dell'utente un'App per la certificazione e generazione della prova dell'età mentre il gestore del servizio può rilasciare un QR Code da utilizzare per inviare la prova direttamente dal proprio dispositivo a maggiore garanzia di segretezza dell'informazione. Spetta all'Autorità il monitoraggio sul rispetto delle regole, a garanzia di un elevato livello di tutela dei minori.

La direttiva è che i meccanismi di verifica non debbano limitare ma favorire la fruizione dei contenuti in rete, che siano facili da usare, tengano conto delle capacità e caratteristiche dei minori e non frappongano inutili ostacoli. Occorre altresì evitare o minimizzare i pregiudizi anche non intenzionali o discriminatori nei confronti di gruppi di utenti. La validità della verifica dell'età deve però cessare nel momento in cui l'utente esce dal servizio o dal browser, se il sistema operativo entra in stand-by e comunque dopo 45 minuti di inattività, per evitare l'accesso altrui senza previa verifica dell'età, se il dispositivo è condiviso con altri. Considerato che tutti i processi sono vulnerabili agli attacchi informatici, spetta agli sviluppatori valutare e prevenire il rischio che un processo non umano sia utilizzato per un attacco a livello di sistema.

Il modello si richiama alle linee guida dell'Autorità francese, cui si ispira la Commissione europea per regolare l'accesso oltre che a contenuti pornografici, a tutti i

⁷³ La riservatezza implica la preclusione del collegamento del servizio con la richiesta della verifica dell'età e il divieto di conservazione dei dati forniti per la verifica da parte del fornitore del servizio di prova dell'età; qualora siano coinvolte terze parti, il divieto si estende a questi ultimi. L'opzione è per una riservatezza rafforzata, che impedisce il riconoscimento dell'utente che ha già utilizzato il servizio al fornitore e alle terze parti che forniscano la prova dell'età o comunque coinvolte nel processo di verifica: Delibera AGCOM, 8 aprile 2025, n. 96/25/CONS, Allegato A, p. 5 ss.

⁷⁴ È questo il primo profilo di anonimato e di riservatezza rafforzata.

⁷⁵ È questo il secondo profilo di anonimato di riservatezza rafforzata.

servizi e attività pericolose e che richiedono una soglia minima di età, legati al gioco d'azzardo, alla vendita di alcolici o tabacco, ad alcuni servizi bancari, per l'accesso ai *social media*. Per questi ultimi è sintomatica l'inversione di tendenza legislativa verso una crescita della soglia minima d'età: pioniere è stato il sistema australiano che ha vietato l'utilizzo dei *social network* da parte dei minori di sedici anni e obbligato i fornitori di *age-restricted social media platforms* ad adottare misure idonee per impedire loro di creare account e accedervi, sanzionando l'inadempimento⁷⁶; *in itinere* è la modifica in Francia per elevare la maggiore età digitale a 15 anni⁷⁷ mentre nel Regno Unito di recente è stato ufficializzato l'intento di elevare a 16 anni il limite d'età⁷⁸. La tendenza trova ulteriori riscontri nelle dichiarazioni di altri governi europei, incluso quello italiano.

La congiuntura tra maggiore età digitale e rigore nei sistemi di verifica dell'età segnala l'intento di riconoscere valenza giuridica al proposito «*not by seeking to protect children from the digital world, but by protecting them within it*», già rappresentato dall'AADC del Regno Unito. In questa ottica si inserisce anche l'obbligo, gravante sui fornitori dei servizi di comunicazione elettronica, di prevedere di *default* e a titolo gratuito sistemi di controllo parentale ovvero un filtro o un blocco dei contenuti inappropriati, disattivabile su richiesta⁷⁹.

6. Il regime sanzionatorio nel sistema integrato di tutele

A completamento del sistema di tutela, il legislatore europeo introduce un modello di responsabilità *ex post* nel contesto delle vulnerabilità dovute alla minore età e identifica la colpa nella violazione dei divieti di cui all'art. 5 *AI Act*. La responsabilità civile grava sul gestore dell'attività pericolosa, ovvero su chi è maggiormente in grado di gestire il rischio di un sistema in sé pericoloso e rappresenta uno strumento di prevenzione integrato con il *risk management*, sanzionando la mancata adozione di misure organizzative conformi alle indicazioni normate a livello europeo; la funzione sanzionatoria, dunque, si aggiunge all'effetto dissuasivo e di deterrenza. Comune è il criterio valutativo, relativo all'adeguatezza dell'assetto amministrativo e operativo a prevenire il danno⁸⁰.

⁷⁶ *Online Safety Amendment (Social Media Minimum Age) Act 2024*, No. 127, 2024, legge con cui sono state apportate modifiche alla precedente legge *Online Safety Amendment 2021*.

⁷⁷ Il disegno di legge n. 2107, *Proposition de loi visant à protéger les mineurs des risques auxquels les expose l'utilisation des réseaux sociaux*, che mira a elevare l'età di accesso ai *social media* a 15 anni, è stato approvato dall'Assemblea nazionale il 27 gennaio 2026 ed è in attesa dell'approvazione del Senato.

⁷⁸ Il premier inglese Starmer il 15 giugno 2026 ha annunciato che entro l'anno sarà approvata la legge che fissa a 16 anni la maggiore età digitale per accedere ai *social network*, legge che entrerà in vigore entro la primavera del 2027 e trasferisce alle piattaforme la responsabilità del controllo.

⁷⁹ Art. 7 bis, d.l. 30 aprile 2020, n. 28, convertito in l. 25 giugno 2020, n. 70. Con la delibera AGCOM 9/23/CONS si è chiarito che per *parental control system* si intende un sistema che permette di limitare o bloccare l'accesso a determinate attività da parte di un minore, impedendo l'accesso, tramite qualunque applicazione, a contenuti inappropriati per la sua età.

⁸⁰ B. MEOLI, *Quali modelli di responsabilità civile nell'era dell'intelligenza artificiale*, in V. D'ANTONIO, B. MEOLI (a cura di), *Responsabilità civile per i danni da intelligenza artificiale*, cit., p. 52.

Le Linee guida della Commissione europea sulle pratiche vietate⁸¹, a carattere esplicativo, riconoscono tutela risarcitoria in presenza di un nesso di causalità ragionevole e plausibile tra la distorsione materiale del comportamento e la tecnica manipolativa, tale da determinare la riduzione della capacità di prendere decisioni informate e autonome, con effetti distorsivi rispetto alle scelte che si sarebbero effettuate con la conoscenza delle informazioni pertinenti, delle opzioni disponibili, dei rischi e benefici connessi. In quanto vulnerabilità endemica, la minore età implica imputazione oggettiva della responsabilità, seppur effetto indiretto di un servizio proposto con finalità di supporto al disagio⁸². La prova liberatoria per l'esonero da responsabilità non verte sulla semplice assenza di colpa, ma richiede l'interruzione del nesso causale tra condotta ed evento dannoso, tratto distintivo della disciplina europea sul trattamento illecito dei dati con il principio di *accountability*. Diversamente se la persuasione opera con trasparenza e rispetto per l'autonomia dell'individuo, quando la finalità è guidare la scelta secondo criteri di razionalità.

Diversi sono i tipi di danno associati alle tecniche manipolative che l'*AI Act* considera significativi: fisici, psicologici, finanziari ed economici, sia se rilevano singolarmente che combinati tra loro.

Il danno fisico comprende ogni lesione o danno alla vita e alla salute della persona, nonché qualsiasi danno materiale ai suoi beni; il divieto, garante della sicurezza dei prodotti, va collegato principalmente ai danni alla vita e salute del minore, per le conseguenze immediate, gravi e irreversibili che determina⁸³. Il danno psicologico riguarda invece gli effetti negativi sulla salute mentale e sul benessere psicologico o emotivo del minore, in genere non immediatamente evidenti ma con conseguenze durature e gravi⁸⁴. Non può escludersi per i minori anche il danno finanziario nella relazione con chatbot che offrono prodotti finanziari fraudolenti, né una combinazione di danni se la lesione fisica provochi anche traumi psicologici, stress, ansia, depressione e viceversa⁸⁵.

Dubbi interpretativi solleva il concetto di danno significativo. La norma richiede che la tecnica sia lesiva di diritti fondamentali, a impatto immediato e diretto ma anche sistemico e indiretto. La minore età dovrebbe rendere il danno significativo *in re ipsa*, a prescindere dalla gravità, dal contesto in cui opera il sistema di IA, dalla portata e intensità degli effetti prodotti, dalla loro durata e non reversibilità⁸⁶. Il rigore interpretativo

⁸¹ Commissione europea, Comunicazione su *Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA)*, Bruxelles, 29.7.2025 C(2025) 5052 final.

⁸² Linee guida sulle pratiche vietate approvate dalla Commissione europea, sezione 3.2.2.

⁸³ Si pensi al *chatbot* che inciti gli utenti all'autolesionismo, al suicidio, ad atti di violenza contro persone singole o minoranze, atti di bullismo o estorsione sessuale.

⁸⁴ Tale tipologia di danno può essere ricorrente in tecniche manipolative che sfruttano le vulnerabilità cognitive ed emotive, come nei sistemi di IA da compagnia capaci di influenzare sentimenti, opinioni o creare rapporti di dipendenza dal servizio, specie se progettati con caratteri antropomorfici.

⁸⁵ Si pensi ad una condizione di stress che provochi insonnia o indebolimento del sistema immunitario.

⁸⁶ Corte di giustizia, sentenza del 7 settembre 2004, *Waddenvereniging e Vogelbeschermingsvereniging*, C-127/02, ECLI:EU:C:2004:482; sentenza dell'11 aprile 2013, *Sweetman e a.*, C-258/11, ECLI:EU:C:2013:220 e Considerando 29 *AI Act*: «Tali sistemi di IA possono essere immessi sul mercato,

proposto consente di rafforzare l'efficacia deterrente della sanzione e di funzionare quale coazione indiretta per l'adozione di misure preventive e di attenuazione dei rischi che gli operatori (fornitore, sviluppatore, *deployer*⁸⁷) devono necessariamente adottare e in modalità adeguata, in ragione della pericolosità dello strumento utilizzato. Un uso responsabile di sistemi sicuri ed etici richiede altresì il costante aggiornamento e adattamento delle pratiche alle regole e prassi più avanzate.

L'inclusione del danno significativo tra le condizioni di rilevanza delle tecniche manipolative mette invece in discussione la configurabilità di un danno *in re ipsa*, insito nella condotta illecita, a prescindere dalla prova di un danno effettivo di natura patrimoniale o non patrimoniale. L'interpretazione restrittiva rappresenta una costante della Corte di giustizia europea nella lesione dei dati personali⁸⁸ ma, secondo un consistente orientamento dottrinale critico, trascura la polifunzionalità che la più recente evoluzione attribuisce all'istituto della responsabilità civile⁸⁹. In particolare, riconoscere nella condotta lesiva un danno *in re ipsa* consentirebbe di valorizzare la deterrenza rispetto alla tradizionale funzione riparativa dell'istituto, strumento più efficace nel contesto di forti asimmetrie digitali e della significativa debolezza tecnologica del minore,

messi in servizio o utilizzati con l'obiettivo o l'effetto di distorcere materialmente il comportamento di una persona e in un modo che provochi o possa verosimilmente provocare a tale persona o a un'altra persona o gruppo di persone un danno significativo, compresi danni che possono essere accumulati nel tempo, e dovrebbero pertanto essere vietati».

⁸⁷ Per *deployer* si intende una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale: art. 3, par. 1, n. 4 AI Act e Linee guida sulle pratiche vietate approvate dalla Commissione europea.

⁸⁸ Corte di giustizia, sentenza del 20 giugno 2024, cause riunite C-182/22 e C-189/22, *JU e SO v. Scalable Capital GmbH*, che sottolinea «Pertanto, l'articolo 82, paragrafo 1, del RGPD è stato interpretato nel senso che il diritto al risarcimento previsto a tale disposizione, segnatamente in caso di danno immateriale, svolge una funzione esclusivamente compensativa, in quanto un risarcimento pecuniario fondato su detta disposizione deve consentire di compensare integralmente il danno concretamente subito a causa della violazione di tale regolamento, e non una funzione dissuasiva o punitiva»; sentenza dell'11 aprile 2024, causa C-741/21, *GP c. juris GmbH*, p. 34 e 35 ove afferma «La Corte ha già interpretato l'articolo 82, paragrafo 1, del RGPD nel senso che la mera violazione del suddetto regolamento non è sufficiente per conferire un diritto al risarcimento, in quanto l'esistenza di un «danno», materiale o immateriale, che sia stato «subito», costituisce una delle condizioni del diritto al risarcimento previsto da tale articolo 82, paragrafo 1, così come l'esistenza di una violazione di detto regolamento e di un nesso di causalità tra tale danno e tale violazione, essendo queste tre condizioni cumulative. Pertanto, la persona che chiede il risarcimento di un danno immateriale sulla base di tale disposizione è tenuta a dimostrare non solo la violazione di disposizioni di detto regolamento, ma anche che tale violazione le ha causato un siffatto danno», ribadendo un orientamento costante con rinvio a Corte di giustizia, sentenza del 25 gennaio 2024, causa C-687/21, *ECLI:EU:C:2024:72*, punti 60 e 61, *MediaMarktSaturn*, e alla giurisprudenza ivi citata.

⁸⁹ E. TOSI, *La tutela risarcitoria della persona nel contesto delle asimmetrie digitali*, cit., p. 47 ss.; V. ROSSI, *Violazione dell'art. 82 GDPR: risarcimento del danno da illecito trattamento di dati*, in *Giurisprudenza italiana*, 2024, n. 4, p. 809 ss.; G.M. RICCIO, *Danni non patrimoniali per violazione dei dati personali: verso un'alluvione giudiziaria?*, in *Foro italiano*, II, IV, 2024, p. 77 ss.; F. CARINGELLA, *In tema di danno non patrimoniale*, ivi, 2024, p. 261 ss.; G. ALPA, *Danno "in re ipsa" e tutela dei diritti fondamentali (diritti della personalità e diritto di proprietà)*, in *Responsabilità civile e previdenza*, 2023, n. 1, p. 6 ss.; G. COLACINO, *"Data breach", danni non patrimoniali e art. 82 g.d.p.r.: il problema della polifunzionalità del rimedio risarcitorio*, in *Rassegna di diritto civile*, n. 7, p. 48 ss.; R. PALMIERI, R. PARDOLESI, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, in *Foro italiano*, 2023, n. 6, IV, p. 278 ss.; U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Rivista di diritto civile*, 2023, n. 3, p. 426 ss.

mentre la prova del danno subito rileverebbe per la quantificazione, laddove non si debba ricorrere a criteri presuntivi o equitativi.

Optare per la sanzionabilità della condotta antigiusuridica in sé accentuerebbe la protezione della vulnerabilità del minore; in quanto condizione sottratta a catalogazioni astratte e uniformi, decisivo diventa il carattere significativo anche di un danno meramente potenziale. La funzione di deterrenza, insita nella sanzionabilità della condotta manipolatrice, lungi dall'introdurre il danno punitivo - inammissibile in assenza di tipizzazione normativa – sarebbe compatibile con la tutela preventiva privilegiata dal legislatore europeo. In altri termini, l'oggettivazione del danno potenzierebbe la funzione deterrente e protettiva della disciplina in quanto valorizza, tra gli elementi costitutivi dell'illecito, la condotta antigiusuridica, dannosa in sé in quanto causa di un danno potenziale, indipendentemente dall'identificazione di un danno reale; diversamente se il servizio digitale ha finalità di persuasione o compensazione di specifiche disabilità, condotta lecita.

Peraltro, la violazione delle disposizioni legislative sulle pratiche vietate consente di sanzionare anche il danno morale soggettivo, la cui valorizzazione si sottrae al criterio compensativo della funzione sanzionatoria, in coerenza con i generali principi di prevenzione e precauzione cui si ispira la disciplina europea della responsabilità civile.

7. Spazio digitale sicuro per i minori: il ruolo dell'asse educativo

L'approccio ambizioso e pionieristico dell'Unione europea con un modello regolamentare di responsabilizzazione *ex ante* e sanzionatorio *ex post* degli operatori inadempienti è tra i più avanzati al mondo, incardinato su principi comuni predisposti per uno sviluppo etico e antropocentrico del mercato digitale e per garantire uno spazio digitale più sicuro e protetto per bambini e adolescenti. Il sistema rafforzato e integrato di protezione risponde al bisogno di contrastare il carattere invasivo delle nuove tecnologie e le potenzialità di condizionamento del processo di crescita e lesivo dei diritti fondamentali di libertà, dignità, salute e riservatezza⁹⁰.

⁹⁰ Il 29 maggio 2026 per la prima volta i ministri del digitale e della tecnologia del G7 hanno concordato sette principi comuni per contribuire a responsabilizzare i bambini, i genitori, e gli educatori in generale, perché i minori possano beneficiare pienamente delle nuove tecnologie, e invitato i fornitori di servizi digitali a tradurre questi principi in azioni. I principi richiedono: l'attuazione di misure efficaci di gestione, valutazione e mitigazione dei rischi, per garantire sicurezza fin dalla progettazione, rafforzate da una trasparenza significativa nella progettazione e sviluppo dei servizi digitali; adozione di soluzioni di assicurazione dell'età robuste, affidabili e che preservano la *privacy*, per supportare esperienze online adeguate all'età per i minori e impedire loro di accedere a servizi digitali limitati all'età; un elevato livello di *privacy* e sicurezza per gli account dei minori, con funzionalità quali i sistemi di raccomandazione progettati per ridurre al minimo l'eccessivo coinvolgimento online, fornendo nel contempo ai minori gli strumenti per avere un maggiore controllo delle loro esperienze online; misure forti per prevenire la generazione, la creazione e la distribuzione, anche attraverso l'IA, di materiale pedopornografico e immagini intime non consensuali, accompagnate da solidi sistemi di sostegno alle vittime; accesso a strumenti parentali semplici, efficaci e interoperabili per genitori e tutori, per aiutarli a supervisionare le attività dei minori online; programmi completi di alfabetizzazione digitale facilmente accessibili da

L'intuizione dominante è la correlazione del *best interest* dei minori con la valorizzazione progressiva dell'autonomia e adattamento dei servizi offerti al livello di indipendenza raggiunto, praticabile tramite ricorso generalizzato a efficaci sistemi di verifica dell'età. Come con i giocattoli analogici educativi, è ipotizzabile differenziare nello spazio digitale servizi adatti ai diversi momenti della crescita, dalla prima alfabetizzazione nell'infanzia e nella scuola primaria, alla fase di transizione durante la scuola secondaria, fino alla prima adolescenza (13-15 anni) e all'avvicinamento all'età adulta con una *compliance by design* meticolosa, inclusiva e capace di adattarsi alle diverse fasi di crescita⁹¹.

L'ambiente digitale sicuro, efficace oltre i confini europei se destinatario è un suo cittadino, rappresenta un precedente logico necessario ma non sufficiente; garantire il diritto di navigare senza subire prevaricazioni, sfruttamento o manipolazioni e il diritto di esprimersi, apprendere e partecipare alla vita digitale presuppone il concorso di attività educative e di vigilanza, che impegna il mondo tecnologico, le istituzioni a cominciare dalla scuola, la famiglia quale contenuto della responsabilità genitoriale. In questo delicato equilibrio non basta monitorare i tempi di utilizzo dei dispositivi, ma individuare i contenuti adatti al reale grado di maturità del minore, percepire situazioni di rischio, cedere il passo quando si riscontra la capacità del minore di comprendere e decidere autonomamente. La vera sfida per mantenere l'intelligenza artificiale, specie generativa, a servizio della persona è riuscire formare una coscienza critica che si evolva con l'età: educare il minore a vivere in un mondo dove la realtà può essere falsificata e aiutarlo a comprendere significa rafforzarlo interiormente, impegno che coinvolge tutti, operatori, istituzioni e genitori, ciascuno nel suo ruolo.

Una realtà complessa e multidimensionale ha bisogno di un approccio sistemico, che implica collaborazione e multidisciplinarietà in sinergia tra aspetti normativi, tecnologici, educativi e culturali, perché nei rapporti con i minori le sfide digitali sono trasversali. Sul piano normativo è *in itinere* in un numero crescente di ordinamenti la modifica della soglia di età per la maturità digitale, da elevare almeno a quindici anni, intervento che resterebbe irrilevante senza un sistema serio di verifica tramite elementi identificatori rigidi (carta di identità o passaporto) magari riservati ai rapporti con le istituzioni, e ricorso all'intermediazione di enti certificati con il sistema del doppio anonimato per i servizi informatici.

genitori, insegnanti e minori, per aiutarli a comprendere meglio i sistemi digitali e a riconoscere i rischi, compresi quelli posti dall'IA generativa; cooperazione tra servizi digitali e ricercatori per consentire la condivisione dei dati con l'obiettivo di migliorare la comprensione dei rischi e rafforzare le soluzioni disponibili per proteggere i minori online.

⁹¹ F. RUGGIERI, *Autonomia e tutela dei minori utenti vulnerabili delle tecnologie digitali*, in C.M. CASCIONE, N. VARDI (a cura di), *Fragilità e innovazione. Rischi e tutele per i soggetti vulnerabili*, Torino, 2025, p. 126. Per l'Autore, l'IA può fornire un significativo apporto per il riconoscimento della crescita e del cambio di esigenze del minore, adattando l'interfaccia, il linguaggio, le impostazioni privacy o anche le specifiche funzionalità dell'oggetto del suo utilizzo, come uno *smart toy* o un *chatbot*, o anche un *social network*, una piattaforma di *e-learning* o una di *streaming*, in quanto capace di un'analisi in tempo reale di grandi quantità di dati, di modo da poter identificare e inibire contenuti o interazioni in grado di costituire un rischio per il minore-utente.

In conformità ai principi europei di proporzionalità, ragionevolezza e precauzione⁹² compete agli operatori che sviluppano modelli generativi e chatbot introdurre opzioni di filtro avanzato dei contenuti, integrando principi etici nei sistemi di intelligenza artificiale, kit che permettano agli sviluppatori terzi di attivare controlli dell'età per l'erogazione dei servizi e maggiore trasparenza algoritmica. Il loro operato deve essere soggetto alla sorveglianza attiva delle Autorità garanti in collaborazione con gli sviluppatori, per identificare *bias* o rischi per i minori, mentre sanzioni esemplari dovrebbero indurre il ridimensionamento dei poteri privati e della sovranità digitale.

Ma un ruolo primario nella responsabilizzazione dei minori è affidato dall'asse educativo, sia tramite l'alfabetizzazione digitale estesa ai genitori magari con meccanismi di consultazione *on demand* su come attivare le protezioni o per consigli semplici, sia soprattutto aiutandoli nello sviluppo della competenza critica che preserva l'autonomia di giudizio insita nella capacità di formulare domande, nucleo irriducibile di ogni esperienza democratica.

In questa prospettiva le misure compensative della vulnerabilità, di competenza di operatori e istituzioni, si dovrebbero integrare con la responsabilità genitoriale nell'ambiente digitale: per essere a misura di minore, il controllo non si esaurisce con l'attivazione di sistemi di *parental control* secondo una logica meramente censoria, né cessa con la maturità digitale. L'approccio flessibile e personalizzato auspicato a livello regolatorio, in attesa di mirati strumenti tecnologici, delega ai genitori il compito di adattare alla personalità individuale la scelta delle metodologie per aiutare i figli nella comprensione della validità e affidabilità delle nuove tecnologie, da utilizzare per migliorare le capacità individuali, senza farsi sostituire nell'errata percezione di confrontarsi con esseri pensanti, onniscienti e infallibili, mentre sono infallibili nella simulazione del pensiero umano. Un impegno complesso seppur non esclusivo, da svolgere con regole precettive o dialettiche in ragione dell'età dei figli, allo stato inevitabile per la sicurezza digitale dei minori, di cui è insidiata non solo la riservatezza ma la crescita equilibrata.

ABSTRACT: Vulnerabilità e minore età, endiadi ricorrente nel quadro normativo europeo per il governo dell'ambiente digitale, vanno percepite come impegno sfidante e non procrastinabile per le legislazioni nazionali. L'osservazione del fenomeno e degli effetti della diffusione non regolamentata dei sistemi di intelligenza artificiale evidenzia un bisogno di protezione non più tarato sul superamento degli ostacoli all'esercizio dei diritti, ma di supporto allo sviluppo dell'identità personale. Il tema non è più la tutela della riservatezza del minore, ma della sua persona, e necessita di un intervento sistemico, con diversi gradi di responsabilità, per coniugare la progressiva conquista di autonomia con le istanze di protezione. In attesa di efficaci

⁹² B. PILEGGI, *I minori sulla rete: un problema di natura costituzionale*, in *BioLaw Journal*, 2024, n. 1, p. 12 ss.

soluzioni tecniche di supporto, la genitorialità è chiamata ad affrontare un compito arduo, che provvedimenti inibitori delle Autorità indipendenti e l'ammissibilità del danno *in re ipsa* potrebbero agevolare.

KEYWORDS: vulnerabilità – minore età – autonomia – responsabilità – personalità.

MINORS' DIGITAL VULNERABILITY AND FORMS OF PROTECTION IN THE EUROPEAN CONTEXT

ABSTRACT: Vulnerability and minor age, a recurring pairing in the European regulatory framework for governing the digital environment, must be viewed as an urgent challenge for national legislation. Observation of this phenomenon and the effects of the unregulated spread of artificial intelligence systems highlights a need for protection no longer focused on overcoming obstacles to the exercise of rights, but rather on supporting the development of personal identity. The issue is no longer the protection of a child's privacy, but rather of the child as a person, which requires a systemic approach, with varying degrees of responsibility, to reconcile the attainment of autonomy with the need for protection. Pending effective technical solutions to support this, parents have a difficult task, but injunction measures by the Independent Authorities and the recognition of damage as *in re ipsa* could facilitate it.

KEYWORDS: Vulnerability – Minors – Autonomy – Responsibility – Personality.