Mimesis Edizioni
Cartografie sociali
www.mimesisedizioni.it

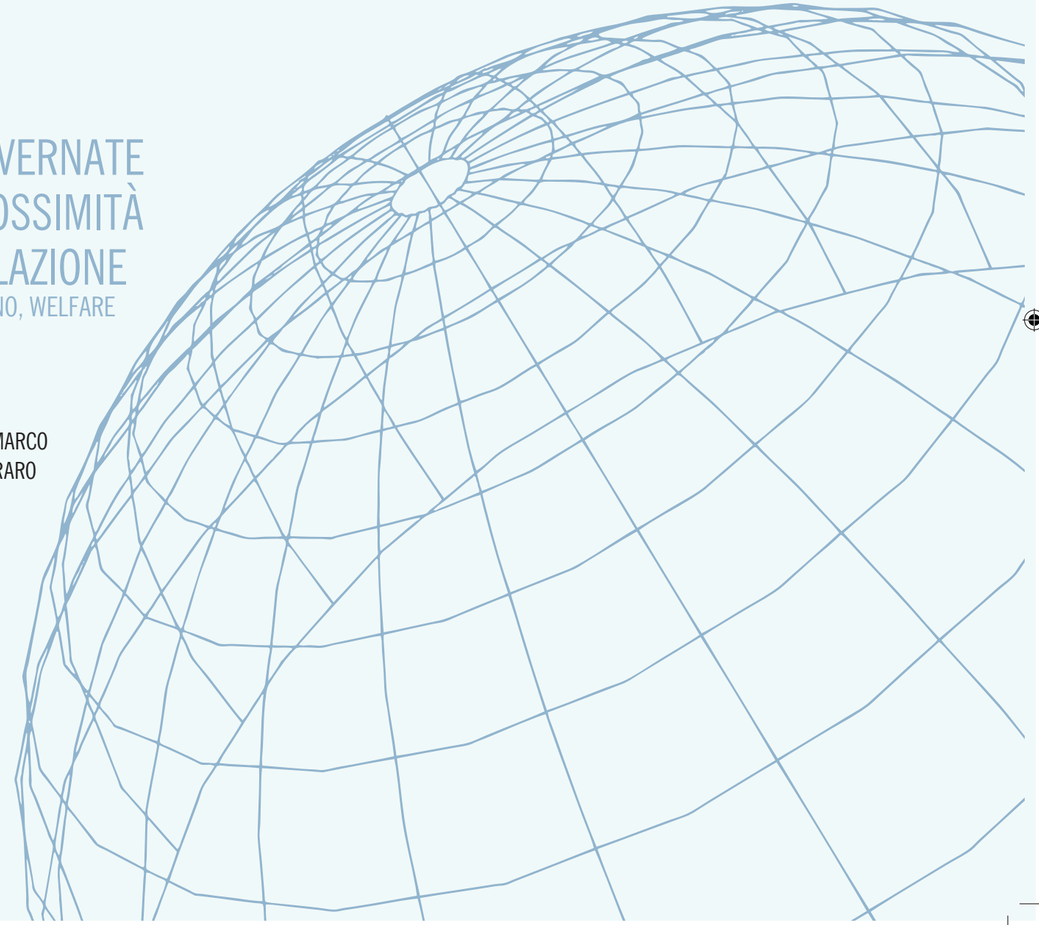
XX,00 euro

ISSN 2499-7641

CARTOGRAFIE SOCIALI
RIVISTA DI SOCIOLOGIA E SCIENZE UMANE
ANNO X, N. 20, 2025
MIMESIS

CARTOGRAFIE SOCIALI

RIVISTA DI SOCIOLOGIA E SCIENZE UMANE ANNO X, N. 20, 2025



VITE GOVERNATE TRA PROSSIMITÀ E REGOLAZIONE

SPAZIO URBANO, WELFARE STATE E DATI

A CURA DI
GIANCARLO DE MARCO
E STEFANIA FERRARO

MIMESIS

CARTOGRAFIE SOCIALI
Rivista di sociologia e scienze umane
Anno X, n. 20, 2025

Direzione scientifica
Lucio d'Alessandro e Antonello Petrillo

Direttore responsabile
Arturo Lando

Redazione
Elena Cennini, Anna D'Ascenzio, Fabrizio Greco

Staff di supporto alla Redazione
Giuseppina Della Sala, Federica Graziano, Luca Manunza, Andrea Postiglione

Staff di supporto alla Redazione per le attività di internazionalizzazione
Lucio Castracani, Laura Giovinazzi

Coordinamento redazionale
Stefania Ferraro (Università degli Studi Suor Orsola Benincasa – Napoli)

Comitato di redazione
Manuel Anselmi (Unitelma Sapienza), Marco Armiero (KTH Royal Institute of Technology, Stockholm),Tugba Basaran (Kent University), Davide Caselli (Università Milano-Bicocca), Valentina Castellini (Università di Toronto), Alberto De Nicola (Alma Mater Studiorum Università di Bologna), Nick Dines (Robert Schuman Centre – European University Institute), Stefania Ferraro (Università degli Studi Suor Orsola Benincasa – Napoli), Marcello Maneri (Università di Milano Bicocca), Alessandro Mazzola (University of Liège), Michelangelo Pascali (Università degli Studi Federico II – Napoli), Domenico Perrotta (Università di Bergamo),Valeria Piro (Università degli Studi di Milano), Ciro Pizzo (Università degli Studi Suor Orsola Benincasa – Napoli), Pietro Saitta (Università di Messina), Luigi Sica (Università degli Studi Suor Orsola Benincasa – Napoli), Anna Simone (Università Roma Tre)

Comitato scientifico
Maurizio Bergamaschi (Alma Mater Studiorum Università di Bologna), Emiliano Bevilacqua (Università del Salento), Fabienne Brion (Université Catholique de Louvain-la-Neuve), Sandro Busso (Università degli Studi di Torino), Alessandro Dal Lago (già professore presso Università di Genova), Davide De Sanctis (Università degli Studi Federico II – Napoli), Vincent Dubois (Université de Strasbourg), Didier Fassin (Institute for Advanced Study School of Social Science, Princeton), Domenico Fruncillo (Università degli Studi di Salerno), Fernando Gil Villa (Universidad de Salamanca), Akhil Gupta (University of California), Michalis Lianos (Université de Rouen), Marco Martiniello (University of Liège), Giulio Moini (Sapienza Università di Roma), Carlotta Mozzana (Università Milano-Bicocca), Laurent Mucchielli (CNRS – Centre national de la recherche scientifique), Fabio Quassoli (Università di Milano Bicocca), Salvatore Palidda (già professore presso Università di Genova), Michel Peraldi (CADIS – Centre d'analyse et d'intervention sociologiques), Andrea Rea (Université libre de Bruxelles), Giuseppe Ricotta (Sapienza Università di Roma), Francesca Vianello (Università degli Studi di Padova)

"Cartografie sociali" is a peer reviewed journal

VITE GOVERNATE TRA PROSSIMITÀ E REGOLAZIONE

Spazio urbano, welfare state e dati

A cura di
Giancarlo De Marco e Stefania Ferraro

MIMESIS

SUOR ORSOLA
UNIVERSITY PRESS

Pubblicazione semestrale: abbonamento annuale (due numeri): € 45,00

Per gli ordini e gli abbonamenti rivolgersi a:
ordini@mimesisedizioni.it
L'acquisto avviene per bonifico intestato a:
MIM Edizioni Srl, Piazza Don Enrico Mapelli, 75
20099 – Sesto San Giovanni (MI)
Unicredit Banca – Milano
IBAN: IT 59 B 02008 01634 000101289368
BIC/SWIFT: UNCRITM1234

Cartografie sociali è una rivista promossa da URiT, Unità di Ricerca sulle Topografie sociali.

Direzione e Redazione della rivista hanno sede
presso l'Università degli Studi Suor Orsola Benincasa
Via Suor Orsola 10 – 80132 Napoli (Italy)
www.unisob.na.it
cartografiesociali@unisob.na.it
cartografiesociali.rivista@gmail.com

UNIVERSITÀ DEGLI STUDI
SUOR ORSOLA
BENINCASA
FACOLTÀ DI
SCIENZE
DELLA FORMAZIONE



MIMESIS EDIZIONI (Milano – Udine)
www.mimesisedizioni.it
mimesis@mimesisedizioni.it

Isbn (Print): 9791222329703
Isbn (Online): 9791222330389
Issn: 2499-7641

This is an open access journal distributed under the terms of the Creative Commons Attribution License (CC BY-4.0).

© 2025 – MIM EDIZIONI SRL
Piazza Don Enrico Mapelli, 75
20099 Sesto San Giovanni (MI)
Phone: +39 02 24861657 / 21100089

Registrazione Tribunale di Napoli n. 37 del 5 luglio 2012

INDICE

Editoriale. microfisica delle comunità: tensioni neoliberali nei processi di controllo e datificazione
di Giancarlo De Marco, Stefania Ferraro 9

MAPPE

Beyond emergency: caivano and the geometries of power amid a crisis-ridden welfare state and the rise of penal governance
di Roberta Basile, Stefania Ferraro 21

Governare la vita attraverso i dati
Per una genealogia della razionalità algoritmica
di Sandro Luce 49

Repressione nel mondo ultrà: la tensione dialettica tra stadio, città e saperi di polizia
di Giancarlo De Marco 67

Consommer l'archétype
Réflexions critiques entre stéréotypes et constructions sociales
di Antonella Emina, Anna D'Ascenzio 93

ROTTE

Una avanguardia culturale?
Realismo capitalista e accelerazionismo di sinistra: concetti chiave e immaginazione sociologica
di Luca Martignani, Davide Dibitonto 111

Dal volontariato al lavoro sociale qualificato: la pandemia da HIV/AIDS come cantiere di professionalizzazione delle associazioni LGBTQIA+ in Italia
di Giusy Paragliola 131

La piattaforma cambia l'arena?
Un'analisi dello spazio partecipativo del forum nazionale per lo sviluppo sostenibile in partecipa
di Tiziana Nupieri 149

I governi della nuova povertà in Europa: sociogenesi comparate
di Federica Graziano 169

RILIEVI

La giustizia riparativa nei reati di genere contro le donne e nella violenza domestica
di Marialaura Cunzio 191

Il terzo settore in presenza di bisogni complessi: criticità dell'esternalizzazione dei servizi a Napoli
di Lucia Cozzolino 209

Modello Toyota e industria 4.0: continuità e punti di rottura
di Barbara Ambrogio 219

Tecnologie dirompenti nei distretti tessili industriali
Un'indagine euristica tra Biella e Reutlingen
di Giancarlo De Marco 229

WUNDERKAMMER

Democrazia più diseguale con l'astensionismo di chi non vuole e chi non può
di Roberto De Luca 259

Dal territorio come spazio al territorio come azione: conflitti e soggettività nel Salento
di Claudia Sabella 263

La scuola delle donne: tra decostruzione, negoziazione e ricostruzione dal basso di linguaggi, teoria e praxis
di Annalaura Ferrara 267

TRAVELOGUES

Social topographies: a reportage from Caivano
di Roberta Basile, Stefania Ferraro 271

Foto-shop
L'evoluzione normativa per la tutela dai Deepfakes al Decreto Caivano e alla Legge 132/2025
di Clara Niola 305

Clara Niola

FOTO-SHOP
L'evoluzione normativa per la tutela dai Deepfakes al Decreto Caivano e alla Legge 132/2025

Abstract:
Every day we post photos and images of ourselves on social media, but are we sure they are not being misused, distorted, or altered? Do we really know the risks we run/face? Do we have the digital skills necessary to protect our digital spaces, our privacy, and our fundamental rights? We are human beings, and our vulnerability grows as the boundaries of cyberspace expand.

Keywords:
Fundamental Rights; Vulnerability; Digital Spaces; Navigation Regulations.

1. *I nuovi diritti dell'era digitale e una maggiore vulnerabilità delle persone*

In un'epoca di lapalissiana evoluzione tecnologica, (anche) attraverso l'utilizzo dell'A.I. (Artificial Intelligent), i confini dello spazio fisico reale si stanno sempre più scomponendo in particelle oscillanti nello spazio virtuale. Le relazioni umane hanno acquistato anch'esse un carattere di a-spazialità e a-temporalità e, nella sovrapposizione tra il reale e il virtuale, si sono resi necessari interventi legislativi per proteggere tutti i fruitori di "Internet", in particolare i minori e altre categorie parimenti vulnerabili dai pericoli del cyberspazio.

Mi piace partire da un contributo di Assunta Mammoliti[1] (invitando il lettore a una lettura dello stesso), la quale definisce il cyberspazio come

> […] un ambiente virtuale creato grazie all'interconnessione di reti digitali, dispositivi (anche mobili) e sistemi informatici e piattaforme di streaming, cloud computing e reti 5G etc, allo scopo di favorire lo scambio di informazioni e interazioni tra gli utenti grazie all'uso dei T.I.C.[2] […] Una nuova dimensione

1 https://www.antiriciclaggiocompliance.it/app/uploads/2025/02/2_Mammoliti.pdf
2 L'acronimo indica la Tecnologia dell'Informazione e della Comunicazione, sviluppata per facilitare il grado e le tecniche di connessione, ampliando ulteriormente il novero degli strumenti.

> sociale, culturale ed economica in cui tutti noi ci muoviamo, comunichiamo e nel quale siamo perpetuamente connessi e spesso vulnerabili […] La vulnerabilità, quale aspetto negativo e non sempre prevedibile dell'interconnessione [...] l'avvento del world wide web[3] [...] una rivoluzione cibernetica, quale nuova scienza, che studia i meccanismi con cui gli uomini comunicano, si muovono e agiscono nell'ambiente esterno […] Una *cyberwarfare* come guerra informatica che sfrutta l'onda costante e innovativa del progresso tecnologico, atta a compromettere la stabilità socio-economica di uno Stato […].

E, tutelare gli utenti dalla propria crescente vulnerabilità dovuta da un utilizzo distorto piuttosto che illecito del WWW, implica l'attuazione di azioni virtuose a opera degli Stati in sinergia con le reti di prossimità quali il "gruppo dei pari", le Scuole, le parrocchie, i Centri sportivi, il Terzo settore ecc.

Ebbene, la *ratio* che ha spinto il Legislatore italiano a numerosi interventi è frutto dell'evoluzione della società e dell'uso delle interconnessioni tecnologiche di cui sopra; non più (e solo) reati informatici – nei quali la condotta tipica della fattispecie legale si arricchisce di elementi costitutivi proprio attraverso l'uso delle nuove tecnologie (ad esempio la frode informatica) – ma anche reati cibernetici, nei quali la commissione della fattispecie legale assume rilevanza giuridica «se commessa in rete o con l'ausilio di uno strumento connesso in rete»[4].

Innanzi a siffatte innovazioni, compaiono anche nuove tipologie di diritti (da tutelare): oltre al già noto diritto alla privacy, si annoverano anche il diritto alla riservatezza informatica, il diritto alla propria identità digitale[5], il diritto all'oblio[6], ancor più avvertito come necessità intrinseca all'umana natura. Il

---

3 Meglio conosciuto con l'acronimo WWW o Web, ovverosia uno dei principali servizi di Internet, che permette di navigare e usufruire di un insieme molto vasto di contenuti multimediali e non, interrelati tramite collegamenti ipertestuali (link) e di fruire di ulteriori servizi accessibili a tutti o a una parte selezionata degli utenti di Internet (mediante autenticazione); in https://it.wikipedia.org/wiki/World_Wide_Web

4 https://www.agendadigitale.eu/documenti/giustizia-digitale/reati-informatici-diritto-penale-dal-computer-crime-al-cybercrime/

5 L'identità digitale, secondo le raccomandazioni dell'AGID, rappresenta lo strumento che permette ai cittadini di identificarsi in modo univoco, come le impronte digitali, da cui l'importanza di inserimento del terzo comma dell'art. 640 ter (furto identità digitale), con la Legge n. 119 del 15 ottobre 2013 in tema di contrasto alla violenza di genere (in G.U. n. 242 del 15 ottobre 2013 - in vigore dal 16 ottobre 2013).

6 «[…] Nel mondo digitale e di Internet, invece, le informazioni possono essere memorizzate, duplicate e condivise con estrema semplicità, con la conseguenza che tutte le informazioni permangono, non ci sono esigenze di selezione, le memorie al silicio sono pressoché illimitate e, nel Cloud, non abbiamo contezza

diritto alla riservatezza informatica, in particolare, viene così innalzato a «diritto fondamentale della persona, diritto a uno spazio informatico esclusivo, che a prescindere dai contenuti che vi siano presenti, trattati o comunicati, deve essere lasciato libero da intrusioni e manomissioni di terzi, in quanto strumento essenziale per la piena realizzazione della persona nell'odierna vita individuale e sociale»[7].

Esso rappresenta un *novum* rispetto al diritto alla privacy, che corrisponde, invece, al diritto a non ricevere intrusioni nella propria vita personale e nei propri dati personali, che potranno essere gestiti e trattati solo previo consenso dell'avente diritto e a determinate condizioni.

Tuttavia, nell'era attuale, riservatezza informatica e privacy devono poter "camminare a braccetto", non potendo l'uno più prescindere dall'altro e, proprio in ragione di siffatta necessità, diventa importante comprendere quali modalità di tutela siano state apprestate dal Legislatore e, in particolare, per i minori e le persone parimenti vulnerabili, soffermando la nostra attenzione sui recenti interventi legislativi. Non da ultimo il Decreto Caivano[8], in tema di "controllo parentale" per i dispositivi di comunicazione elettronica, in materia di ulteriore modalità di prevenzione e di «contrasto alla povertà educativa, quale possibile preludio al disagio giovanile, alla criminalità minorile, anche in ambito digitale».

Il mondo è in piena evoluzione e i ragazzi tra gli 11 e i 17 anni sono sempre più digitali. Infatti, secondo un Report ISTAT 2024 è cresciuto dell'85% il numero dei giovani che possiede un profilo *social network*, con una differenza di genere a favore delle ragazze, anzitempo connesse rispetto al gruppo dei propri pari:

> per queste generazioni anche le relazioni con gli amici passano attraverso Internet. L'8,4% dei giovanissimi dice di essere continuamente online o al telefono con gli amici (chat, chiamate, videochiamate, ecc.). Il 40,3% dichiara di essere online o al telefono con amici più volte al giorno[9].

---

concreta di chi e dove ha memorizzato, duplicato, indicizzato e pubblicato le nostre informazioni. L'esigenza oggi non è quella di avere memoria, di ricordare delle informazioni ma, piuttosto, di dimenticare»; in https://www.agendadigitale.eu/sicurezza/privacy/il-diritto-alloblio, di Anna Cataleta, Senior Partner di P4I e Senior Advisor presso l'Osservatorio Cybersecurity & Data Protection (MIP).

7 https://www.aipdp.it/allegato_prodotti/115_001_Reati_informatici_e_contro_riservatezza_Picotti.pdf

8 D.L. n. 123 del 15 settembre 2023 (entrato in vigore il 16 settembre 2023 - G.U. n. 216 del 15/09/2023) e convertito con modificazioni nella Legge n. 159 del 14 novembre 2024 (G.U. n. 266 del 14/11/2023).

9 https://www.istat.it/wp-content/uploads/2024/05/Bambini-e-ragazzi-2023.pdf

Nel Report 2025, inoltre, viene rilevato come il nostro Paese si trovi al di sotto della media europea proprio in tema di competenze digitali di base, così evidenziando come il divario sia sempre fortemente associato al genere, all'età, al livello di istruzione e alla "disparità territoriale" tra Nord-Centro e Mezzogiorno:

> […] le competenze digitali restano insufficienti […] Nel 2023 solo il 45,8 per cento degli italiani tra i 16 e i 74 anni possiede competenze digitali almeno di base, contro una media UE del 55,5 per cento e obiettivi europei che puntano all'80 per cento entro il 2030 [...][10].

2. *La tutela del minore nell'era digitale: il control parental e il consenso*

Al netto di una irrefrenabile evoluzione digitale (cyberspazio e metaverso[11]), appare evidente come il garantire un'istruzione digitale di base tra la popolazione adulta – considerando proprio quell'aspetto negativo e non sempre prevedibile della "vulnerabilità" dell'interconnessione ex-Mammoliti – abbia significato rivolgere maggiore attenzione ai minori e ad altri soggetti parimente deboli, non ancora padroni di una "navigazione digitale" pienamente consapevole e responsabile.

A tal fine, nel Decreto Caivano è stato previsto l'uso di applicazioni che consentono un controllo parentale; in particolare, l'art. 13 co. I lett. a) e c) ci offre definizioni di carattere generale:

> [...]
> a) controllo parentale: la possibilità di limitare e controllare, da parte dei genitori o di coloro che esercitano la responsabilità genitoriale, l'accesso ai contenuti e/o alla rete da parte dei minori, mediante la scelta degli spazi digitali e dei tempi di utilizzo; [...]
> c) applicazioni di controllo parentale: elementi esterni a dispositivi di comunicazione elettronica, soluzioni a livello di rete o applicazioni o software per dispositivi di comunicazione elettronica, facilmente comprensibili e accessibili agli utenti, che consentano il controllo parentale [...].

10 https://www.istat.it/wp-content/uploads/2025/05/R-Annuale-2025-integrale.pdf

11 Per semplicità, ripropongo il significato di metaverso della rivista on-line *Money.it*, in cui si legge che «trattasi di ambienti virtuali tridimensionali e persistenti, dove gli utenti possono interagire, lavorare, apprendere e consumare in modalità immersiva, spesso attraverso avatar personalizzati e dispositivi di realtà virtuale». Per chi volesse approfondire, https://www.money.it/metaverso-cos-e-come-funziona-e-come-si-entra.

Innalzare la quota della popolazione di età compresa tra 16 e 74 anni con competenze digitali di base risulta, quindi, uno degli obiettivi del programma strategico UE per il decennio digitale da attuare con una certa priorità.

Con la Decisione del Parlamento europeo e del Consiglio del 14 dicembre 2022, n. 2481 l'Unione Europea[12] – sottolineando l'importanza di «un rispetto dei diritti fondamentali della persona […] della sicurezza […] della qualità della vita» (Considerando 1) e rimarcando l'obbligo per gli Stati membri, nei settori i cui progressi sono ritenuti insufficienti, di «compiere passi avanti verso il conseguimento degli obiettivi digitali in linea con le traiettorie previste […] proponendo l'adeguamento delle politiche, delle misure e delle azioni che intendono intraprendere per favorire i progressi nel settore critico di cui in questione» (Considerando 35) – ci offre una definizione di competenze digitali di base (art. 2, punto 10)[13], evidenziando un distinguo rispetto al comma precedente in tema di competenze digitali avanzate (art. 2, punto 9)[14].

Sommessamente, mi pongo l'interrogativo se le prime possano essere sufficienti a raggiungere quello scopo di prevenzione cui la norma mira, poiché l'utente ultimo – pur non essendo fornito di quelle specifiche competenze al pari di un gestore/creatore della piattaforma – comunque utilizza e gestisce (*latu sensu*) delle tecnologie senza avere quella competenza specifica necessaria, con l'alto rischio di commettere illeciti piuttosto che non possedere gli strumenti idonei alla propria tutela.

Ne consegue che proprio attraverso un uso improprio, cioè distorto del *network* (voluto ovvero dovuto per colpa generica, specifica o colpa cosciente) e di tutti i "dati" e i contenuti esistenti, ovvero attraverso una loro manipolazione, si possano arrecare danni irreversibili (esiste realmente un diritto all'oblio?), per cui disquisire della necessità di una tutela del minore, piuttosto che di una sua responsabilità, piuttosto che di quella dell'adulto di riferimento, dei gestori delle piattaforme e di altre parti a vario titolo coinvolte, significa cercare di comprendere tutte quelle situazioni concatenate e correlate tra loro, la cui tutela ha imposto ai Legislatori nazionali e sovranazionali il bilanciamento di tanti diritti e doveri, la cui analisi ha chiamato in causa tutte le professionalità diversamente coinvolte.

12 https://eur-lex.europa.eu/eli/dec/2022/2481/oj?locale=it.

13 Competenze digitali di base: la capacità di svolgere con mezzi digitali almeno un'attività connessa ai seguenti settori: informazione, comunicazione e collaborazione, creazione di contenuti, sicurezza e dati personali, risoluzione di problemi.

14 Competenze digitali avanzate: le abilità e le competenze professionali che richiedono le conoscenze e l'esperienza necessarie per comprendere, progettare, sviluppare, gestire, testare, implementare, utilizzare e mantenere le tecnologie, i prodotti e i servizi digitali.

È in questa prospettiva, al fine precipuo di garantire un ambiente digitale sempre più sicuro, che si è giunti all'emanazione della Legge 23 settembre 2025 n. 132, con la quale[15] – uniformandosi alle disposizioni del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 – il Legislatore ha «promosso un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità. Garantisce la vigilanza [...] sull'impatto sui diritti fondamentali dell'intelligenza artificiale» (art. 1, L. 132/2025).

Il richiamo immediato di conformità al Regolamento UE[16] assume rilievo laddove la normativa europea, offrendo regole di classificazione dei sistemi di A.I.[17] "ad alto rischio"[18] (art. 6), pone subito al centro della tutela «[…] la salute, la sicurezza o l'impatto negativo sui diritti fondamentali delle persone fisiche, anche nel senso di influenzare materialmente il risultato del processo decisionale […]; la portata potenziale del danno e/o dell'impatto negativo deve essere valutato in termini di intensità e capacità di incidere su più persone o di incidere in modo sproporzionato su un particolare gruppo di persone (art. 7)». Inoltre, attribuisce importanza a una supervisione e a una sorveglianza dell'essere umano, attraverso «[…] strumenti di interfaccia uomo-macchina adeguati», in modo tale da poter «essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso, e sempre per prevenire e o ridurre al minimo i rischi per la salute, la sicurezza e per tutti i diritti fondamentali» della persona che le nuove tecnologie digitali – tra cui l'A.I., il 5G, il cloud, l'*edge computing*[19] e internet – hanno coniato (art. 14).

Con il presente contributo, si cercherà quindi di analizzare quella parte di normativa ritenuta basilare (ma per nulla esaustiva) al fine di tutelare i minori e le altre persone parimenti vulnerabili dai pericoli sottesi ai c.d. *Deepfake* attraverso il sistema di intelligenza artificiale. I *Deepfake*[20] rappresentano una

15 G.U. n. 223 del 25 settembre 2025 ed entrata in vigore il 10 ottobre 2025.

16 https://eur-lex.europa.eu/eli/reg/2024/1689/oj

17 Art. 3, punto 1, Regolamento (UE), «un sistema automatizzato, progettato per funzionare con livelli di autonomia variabile e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che ricevere come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

18 Art. 3 punto 2 Regolamento (UE), «rischio: la combinazione delle probabilità del verificarsi di un danno e la gravità del danno stesso».

19 «L'edge computing è un modello di calcolo distribuito nel quale l'elaborazione dei dati avviene il più vicino possibile a dove i dati vengono generati, migliorando i tempi di risposta e risparmiando sulla larghezza di banda [...]», in https://it.wikipedia.org/wiki/Edge_computing.

20 La tecnica in questione si è sviluppata inizialmente nell'ambito della ricerca accademica e, successivamente, nelle comunità online a livello amatoriale. Un progetto pionieristico in questo ambito fu il *Video Rewrite*, pubblicato nel 1997,

tecnologia già esistente da tempo, affascinante e quantomai pericolosa che consistono in *media* (ossia immagini o video o altro) reali e/o fittizi attraverso la sovrapposizione e/o combinazione di altri *media*, elaborati grazie all'uso di reti neurali che, usate come *machine/deep learning*, sono in grado di elaborare/rigenerare i dati creando nuovi contenuti digitali. Le creazioni virtuali tanto possono essere generate *ex-novo* tanto da immagini/video già esistenti, modificate e alterate, così da sembrare veritiere attraverso i sistemi di intelligenza artificiale.

Siffatta tecnologia si basa sull'uso di una rete neurale che, al pari del cervello umano, è in grado di elaborare i dati di partenza con quelli che già circolano in rete, migliorando i dati acquisiti e la propria capacità di autoapprendimento. È apparso subito evidente come, attraverso la diffusione e un uso improprio/illecito di creazioni, alterazioni e/o modificazioni di *dati*, possono venir lesi i diritti fondamentali delle persone (anche quelli di nuovo conio), così che il Legislatore si è dovuto adeguare nella previsione di una nuova fattispecie di reato, non potendo più convogliare queste nuove condotte nell'alveo di quelli già esistenti.

Ebbene, proprio immaginando un utilizzo da parte dei minori dell'A.I., di profili *fake,* di *App* idonee ad alterare immagini/video che circolano *in etere,* nonché di altre tipologie di "dati", il richiamo all'art. 13 Decreto Caivano in tema di *parental control* appare quantomai opportuno, proprio per sottolineare la necessità di un obbligo di controllo e di sorveglianza (*rectius*: responsabilità) anche in capo agli adulti di riferimento.

La giurisprudenza è, in più occasioni, intervenuta ante *riforma* L. 132/2025 come quando (Tribunale di Brescia, sentenza del 4 marzo 2025, n. 879) ha condannato dei genitori al risarcimento dei danni in relazione all'apertura di un profilo Instagram da parte del loro figlio, ma apparentemente riconducibile a un'ignara vittima e riproducente contenuti a carattere intimidatorio, minacciosi, offensivi con pubblicazione di fotografie sessualmente esplicite. In tale pronuncia, invero, il collegio – non potendo perseguire il reale autore «perché incapace di intendere e di volere al momento del compimento del fatto» – sotto il profilo civile, ha ritenuto responsabili i genitori ex-art. 2047 c.c.:

---

che consisteva nella modifica di un video esistente di una persona mentre parla, facendola apparire come se stesse pronunciando parole diverse da quelle originali. Nel 2017, un utente di Reddit, con lo pseudonimo *deepfakes*, diede il nome a questa tecnologia il cui significato deriva dall'unione dalle parole *fake* (falso) e *deep*, a sua volta riferito al *deep learning*, cioè intelligenza artificiale; cfr. M. Carosi, *Profili del nuovo reato ex art. 612-quater c.p.*, 10 ottobre 2025, https://www.giuridicamente.com/l/reato-deepfake-art-612-quater-cp/.

> […] ché erano tenuti alla vigilanza della figlia la cui incapacità era pacifica e ben nota […] inosservanza del dovere di vigilanza del soggetto incapace […] dal momento che gli accorgimenti da loro predisposti con riferimento all'utilizzo dei social network non possono ritenersi sufficienti […] neppure la mancanza di competenze tecno-informatiche per verificare l'eventuale esistenza di profili fake che non risultino dal profilo ufficiale salvato su di un dispositivo […][21].

L'A.G. si è espressa nel sottolineare come i genitori/gli adulti di riferimento, pur se inesperti in campo tecnico-informatico, hanno il dovere di acquisire un livello minimo di competenze digitali e informatiche attraverso *tutorial*, percorsi di studi ecc…; e a informarsi attivamente sui mezzi tecnologici utilizzati dai loro figli e sui relativi rischi, migliorando tali competenze attraverso spazi dedicati all'educazione digitale per contrastare fenomeni emergenti, come per esempio il *sexting*[22], il *morphing*[23], il *doxing*[24] e lo *sharenting*[25].

Se ci riflettiamo, al Considerando 12 della Decisione (UE) 2022/2481 *ut supra* citata, il Parlamento europeo e il Consiglio avevano già sottolineato l'importanza di una educazione digitale del minore specificando che, per conseguire tutti gli obiettivi prefissati nei diversi settori presi in considerazione, «sarebbe necessario concentrarsi sull'istruzione, al fine di garantire che la comunità dell'istruzione, in particolare gli insegnanti, sia adeguatamente formata, educante e in grado di utilizzare la tecnologia in modo efficace nei propri metodi didattici e di insegnare l'uso delle tecnologie digitali, affinché gli studenti siano meglio preparati [...]». Istruzione e Formazione in campo digitale sono le due parole chiave per consentire un uso consapevole e responsabile della tecnologia, per aumentare l'alfabetizzazione mediatica e digitale, onde prevenire i rischi connessi a un uso improprio e irresponsabile della tecnolo-

21 https://www.sugamele.it/misc/news/attachments/4/NEWS-ALLEGATO-SENTENZA-0-20976.pdf?srsltid=AfmBOoq49VznvOLzSeQizHhr6H2O30IbQl44BEKlGfGPKlAEGp8mwWQU

22 Consiste nella realizzazione di immagini o video che hanno per oggetto la vita privata sessuale di un minore, che abbia raggiunto l'età del consenso sessuale nell'ambito di un rapporto tra pari: fattispecie che non costituisce necessariamente reato se esso è frutto di una libera scelta e destinato a un uso strettamente privato (in, SS.UU. Sent. 51815 del 31 maggio 2018, M., Riv. 274087-02).

23 Consiste nell'alterazione digitale di volti, forme, corpo o altri oggetti.

24 Consiste nel diffondere informazioni di dati sensibili relativi ad altro soggetto, attraverso internet, allo scopo di intimidirla, minacciarla. In https://www.altalex.com/guide/doxxing

25 Consiste nella diffusione sui *social* delle immagini e/o video dei minori da parte dei genitori: *share* sta per condividere sui *social*, mentre *parenting* significa "fare i genitori".

gia da parte anche di quei soggetti (gli adulti di riferimento) che dovrebbero, *ex-lege*, provvedere alla tutela dell'ordinario sviluppo psico-fisico del minore.

Non a caso, la necessità di recuperare il Report Istat 2025 serve a evidenziare come il nostro Paese si trovi al di sotto della media europea in tema di competenze digitali di base, sottolineando – implicitamente – l'importanza di una educazione digitale delle stesse famiglie che verrà, per l'appunto, richiamata, nel sesto Piano nazionale di azione e di interventi per la tutela dei diritti dei soggetti in età evolutiva 2025-2027.

Innanzi a questo *mare magnum*, diversi sono stati gli *step* per la realizzazione di una disciplina unitaria a tutela dei diritti fondamentali della persona. Se ci riflettiamo, già nel 2003, con l'emanazione del Codice della Privacy[26], si era cominciato a discutere circa il corretto utilizzo (*rectius*: trattamento) dei dati personali nel rispetto dei diritti e delle libertà fondamentali, sottoponendo all'attenzione dei lettori anche un utilizzo di terminologie specifiche. Entrano, così, nel lessico quotidiano dei lemmi con significati *ad hoc* come trattamento[27], dati personali[28], dati sensibili[29], dati giudiziari[30], titolare del trattamento[31], responsabile del trattamento[32].

---

26 D. Lgs n. 196 del 30 giugno 2003, G.U. n. 174 del 29 luglio 2003 - supplemento ordinario n. 123.

27 Inteso come qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

28 Inteso come qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

29 Intesi come quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

30 Intesi come quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del cp.p.

31 Definita come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

32 Definita come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposti dal titolare al trattamento

Successivamente, con il GDPR[33] (Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, aggiornato alle rettifiche GUUE n. 127 del 23 maggio 2018), è stato predisposto un incremento di tutela per la protezione del trattamento dei dati a carattere personale. Per quanto concerne il trattamento dei dati personali dei minori, quali soggetti maggiormente vulnerabili, è stato espressamente previsto, al Considerando 18, che «quantunque il presente regolamento non si applichi nell'ambito di attività a carattere personale o domestico ivi comprendendo anche l'uso dei social network, esso si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare i dati personali nell'ambito di tali attività a carattere personale o domestico».

Insomma, laddove il trattamento dei dati personali avvenga già rispettando una o tutte le condizioni previste ex-art. 6, par. 1, lett. a) del GDPR 2018 da parte dei titolari/responsabili che forniscono i mezzi per trattare i dati personali, «il trattamento dei dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età minore ai 16, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare delle responsabilità genitoriale. Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni» (art. 8, co. I, GDPR 2018)[34].

Emerge inesorabile l'importanza del "consenso" da intendersi come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso [...] che i dati personali che lo riguardano siano oggetto di trattamento» (art. 4, Regolamento (UE) 2016/679). D'altronde, già al Considerando 38, proprio sottolineando lo *status* di vulnerabilità dei minori, in maniera ancora più peculiare, si anticipa la *ratio* di tutela:

> I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe

di dati personali.

33 L'acronimo sta per *General Data Protection Regulation*.

34 https://eur-lex.europa.eu/IT/legal-content/summary/general-data-protection-regulation-gdpr.html.

essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.

Insomma, per poter trattare i dati personali dei minori (o, comunque, di un soggetto parimenti vulnerabile) occorre un consenso lecitamente espresso dal titolare del dato stesso (sempreché abbia l'età legale per poterlo esprimere) piuttosto che da coloro che esercitano la responsabilità *ex-natura* piuttosto che *ex-lege* nei confronti degli stessi.

In Italia, i limiti d'età stabiliti per esprimere un valido consenso al trattamento dei propri dati personali sono fissati nel D. Lgs del 10 agosto 2018 n. 101[35], attraverso l'inserimento, nella parte I, Titolo I del Codice Privacy 2003, dell'art. 2 quinquies[36], secondo il quale «il minore che abbia compiuto i 14 anni può "trattare" i propri dati personali» con l'uso di un social network; se infra-quattordicenne, invece, occorre il consenso genitoriale ai sensi dell'art. 6, par. 1, lett. a, GDPR.

È bene precisare che, in ordine all'adeguamento della "congrua età" per esprimere un consenso, anche l'Autorità Garante per l'Infanzia e l'Adolescenza (AGIA) fu chiamata a esprimere un parere[37], dopo aver interpellato esperti delle varie professionalità a vario titolo coinvolti (psicologi, giuristi, pedagogisti, tecnici della comunicazione); così, con parere n. 1008 del 24 aprile 2018, fu precisato che non esistono criteri rigidi per poter affermare "quando" un minore sia consapevole e responsabile per esprimere il proprio consenso digitale, poiché l'età anagrafica può soltanto essere uno degli indici da poter tenere in considerazione, in quanto la consapevolezza è strettamente legata alla maturazione individuale e all'educazione specifica ricevuta. L'AGIA si espresse così, per la prima volta, ritenendo fondamentale divulgare una alfabetizzazione

35 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129); entrata in vigore 19 settembre 2018- G.U. n. 205 del 04/09/2018.

36 Art. 2-quinquies (Consenso del minore in relazione ai servizi della società dell'informazione). 1. 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.

37 https://www.garanteinfanzia.org/sites/default/files/parere-schema-decreto-regolamento-2016-679-ue.pdf

digitale per far sì che il minore potesse comprendere tutte le implicazioni di ordine giuridico, economico, sociale, che quel *clic* o quel *mi piace* può produrre. Lo stesso organo monocratico – per richiamare il Regolamento europeo 2016/679/UE circa il compimento del 16 anno di età per esprimere un consenso digitale da parte del minore – ebbe a recuperare una serie di norme che, in deroga alla regola generale stabilita dal codice civile secondo cui «la capacità di agire si acquisisce col compimento del diciottesimo anno di età» (art. 2 c.c.), riconosce al minore che abbia compiuto 16 anni una serie di facoltà/capacità tra cui l'ingresso nel mondo del lavoro e la capacità a prestare il consenso per la pubblicazione della propria immagine.

Insomma, l'AGIA ritenne che sarebbe stato meglio «rispettare la soglia dei 16 anni» per consentire ai minori di poter esprimere un proprio consenso digitale, presentando gli stessi una maggiore capacità di discernimento e di autodeterminazione. Nel suo contributo, concluse con una chiosa ritenuta fondamentale: «[…] altresì che spetti alle Istituzioni e alle Agenzie educative la predisposizione di programmi formativi idonei a costruire una adeguata consapevolezza digitale […]».

3. *Il Piano nazionale di azione e di interventi per la tutela dei diritti dei soggetti in età evolutiva 2025-2027 e il Decreto Caivano: l'age verification*

Se già nel 2018 si era avvertita la necessità di promuovere un'educazione digitale, oggi, è divenuta uno dei pilastri dell'area di intervento da parte del Legislatore italiano che ha sottolineato l'importanza del

> prendersi cura dei minori con un approccio innovativo e inclusivo. All'infanzia ed all'adolescenza non ci si approccia come a una questione di cui occuparsi soltanto in presenza di disagi […] l'approccio sussidiario e non verticistico, che mette al centro le istanze dei territori e ne valorizza le buone pratiche realizzate in un'ottica non assistenziale, ma solidale e partecipativa; la centralità della famiglia, attorno alla cui responsabilità deve ruotare l'universo educativo e relazionale dei minori [...][38].

Per giungere a realizzare uno sviluppo armonico di tutti gli aspetti che riguardano i minori, diverse sono state le aree di intervento prese in considera-

38 https://www.famiglia.governo.it/media/33jj5zud/piano_famiglia_2025_2027.pdf; sesto Piano nazionale per la famiglia e del Piano nazionale di azione e di interventi per la tutela dei diritti dei soggetti in età evolutiva 2025-2027; *Prefazione*, Eugenia Roccella, Ministra per la famiglia, la natalità e le pari opportunità, Roma, 2-3 ottobre 2025.

zione, in sinergia con una rete di prossimità (famiglia, scuola, comunità dei pari, associazioni culturali e sportive, terzo settore); si evince la necessità

> […] di realizzare percorsi di sensibilizzazione e informazione in ambito scolastico rivolti ai ragazzi ed alla comunità scolastica ed al Centro per le famiglie, in sinergia con gli altri luoghi e servizi territoriali di prossimità, per meglio imparare a gestire le sfide che il mondo dell'A.I. ci propone nella nostra quotidianità [...][39].

L'uso consapevole di un *social networ*k da parte dei minori, così come la necessità di una divulgazione dell'alfabetizzazione digitale a partire dalle famiglie – congiuntamente all'adozione da parte dei gestori delle piattaforme di misure adeguate a proteggere i minori da contenuti dannosi piuttosto che inappropriati – costituisce la base di conoscenza per evitare che, attraverso un uso distorto dell'A.I., si pongano in essere condotte di *Deepfake* piuttosto che delle più gravi *Deep nude*. La promozione dell'educazione digitale parentale, di cui ha parlato l'AGIA nel 2018, poi ripresa anche dall'U.E. nella Decisione 2481/2022, ritorna a essere uno dei capisaldi delle politiche di intervento per la tutela dei diritti e lo sviluppo dei minori nell'ambito del Piano per le Famiglie 2025-2027.

A testimonianza di questa politica d'intervento integrata, già con la Delibera del 25 gennaio 2023 n. 9/23 CONS, l'AGCOM (Autorità Garante nelle Comunicazioni) aveva adottato le Linee Guida finalizzate all'attuazione dell'art. 7-bis del Decreto-Legge 30 aprile 2020 n. 28 in materia di «sistemi di protezione dei minori dai rischi del cyberspazio»[40], così garantendo l'attuazione del controllo parentale come ulteriore sistema di vigilanza delle fasce vulnerabili dai rischi del Web e da un uso distorto dell'A.I..

E, infatti, l'Autorità Garante nelle Comunicazioni, dopo la consultazione con tutti i protagonisti socio-giuridico-economici a vario titolo coinvolti, aveva vincolato i fornitori dei servizi di comunicazione a offrire informazioni trasparenti, adeguate e aggiornate proprio «in merito alla disponibilità ed al corretto utilizzo del servizio fornito», lasciando loro la libera modalità di

39 *Ibidem*.

40 L'art. 7-bis del decreto-legge 30 aprile 2020, n. 28, rubricato «Sistemi di protezione dei minori dai rischi del cyberspazio», dispone quanto segue: 1. I contratti di fornitura nei servizi di comunicazione elettronica disciplinati dal codice di cui al decreto legislativo 1° agosto 2003, n. 259, devono prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati a un pubblico di età superiore agli anni diciotto. 2. I servizi preattivati di cui al comma 1 sono gratuiti e disattivabili solo su richiesta del consumatore, titolare del contratto.

realizzazione degli stessi con una chiosa: le Linee Guida dovevano (e devono) individuare soltanto i requisiti minimi e opzionali dei sistemi di *parental control* rilasciati dagli stessi. Le Linee Guida[41], infatti, forniscono indicazioni sulle categorie e sui contenuti da bloccare secondo ambiti generali di applicazione (per esempio: pornografia, gioco d'azzardo, violenza, sesso, razzismo, scommesse) lasciando la libertà ai fornitori stessi di ampliare l'elenco (non tassativo) di altri contenuti.

L'importanza delle summenzionate Linee Guida si evince anche sul piano pratico: il mancato utilizzo del *parental control* espone i genitori, ovvero altri soggetti responsabili dell'educazione e della regolare crescita del minore, a una *culpa in vigilando* (da intendersi come carenza di vigilanza che ha consentito/permesso al minore di compiere un illecito piuttosto che accedere a un contenuto nocivo. Il fatto dannoso, allora, è la conseguenza della inadeguata ovvero omessa vigilanza da parte degli organi di sorveglianza) e una *culpa in educando* (da intendersi quale carenza nell'educazione impartita, che non è stata sufficiente a prevenire gli illeciti ovvero l'accesso a contenuti nocivi da parte del minore ovvero danni a terzi)[42].

Interessante notare, guardando a un passato non troppo lontano, come anche la giurisprudenza abbia sottolineato, in più occasioni, l'importanza della supervisione da parte degli adulti di riferimento del cellulare dei minori, dei contenuti che gli stessi scaricano, ovvero immettono in rete, così dimostrando sempre maggiore aderenza della legge alla realtà. A tal proposito, degna di attenzione la sentenza del 05 agosto 2020 n. 698 con la quale il Tribunale civile di Parma aveva previsto espressamente che

> [...] i contenuti presenti sui telefoni cellulari dei minori andranno costantemente supervisionati da entrambi i genitori, evitando la comparsa di materiali non adatti all'età ed alla formazione educativa dei minori. La stessa regola vale per l'utilizzo eventuale del computer, al quale andranno applicati i necessari dispositivi di filtro [...].

Senza con ciò limitare alcuna forma di sviluppo della personalità del minore e della correlata necessità di socializzazione.

41 https://www.agcom.it/sites/default/files/migration/delibera/Delibera%209-23-CIR.pdf

42 Il fondamento giuridico della *culpa in educando* va ricercato nell'art. 2048 c.c., secondo il quale «i genitori sono responsabili dei danni cagionati dai figli minori salvo che provino di non aver potuto impedire il fatto»; così come anche la *culpa in vigilando* trova fondamento nell'art. 2048 c.c., oltre che nella regola generale del *neminem laedere* ex-art. 2043 c.c..

Sulla stessa linea, la più recente sentenza del 10 marzo 2025 n. 304 con cui il Tribunale civile di Termine Imerese ha ritenuto responsabili dei genitori (e anche dei ragazzi, che nelle more erano divenuti maggiorenni) per aver creato una pagina *on line* diffamatoria e denigrante nei confronti di una coetanea: pagina rimasta attiva fini all'intervento dell'Autorità Giudiziaria. Anche in quest'ultima vicenda, la responsabilità dei genitori ex art. 2048 c.c. è stata considerata diretta e fondata sulla *culpa in vigilando* a causa della condotta (dato fattuale) posta in essere dai figli, con un *quid pluris*: il grado di vigilanza dei genitori doveva essere modulato e proporzionato non solo all'età anagrafica dei figli, ma tenendo in considerazione il concreto sviluppo psico-fisico dei minori, l'assenza di malattie ritardanti, la forza del carattere e la capacità degli stessi di rendersi conto del disvalore e dell'illeceità della propria azione.

Si badi, però, che l'attività di vigilanza e controllo deve avvenire rispettando la privacy del figlio, diritto che può esser limitato laddove l'adulto di riferimento si renda conto che il minore non abbia effettivamente assimilato i comuni valori e regole del vivere in comunità, per cui solo allora «sarebbe possibile giustificare una loro intrusione nella sfera privata del minore attraverso l'attività di vigilanza e controllo» (Cass. Pen., Sez. V, sentenza del 19 gennaio 2024 n. 7470)[43].

A ogni modo, è evidente che per il genitore/adulto di riferimento non è sufficiente dimostrare di aver dato delle mere raccomandazioni piuttosto che spiegazioni (seppur continue e specifiche) sui pericoli del Web e sull'uso distorto dello stesso per poter ritenersi esonerato da responsabilità, giacché «se il minore riesce a eludere la sorveglianza ed a compiere, comunque, atti illeciti, ciò sta a significare che quella forma di vigilanza non è adeguata neppure nella sua intensità»[44]. Emerge, quindi, l'importanza dell'attivazione del *control parental*, quale una delle regole basilari da seguire onde evitare che qualsivoglia contenuto lesivo e dannoso possa essere immesso in rete piuttosto che manipolato. Il controllo parentale deve poter, quindi, essere configurato e disattivato attraverso procedure semplici e intuitive come, per esempio, l'uso dello SPID, di un codice PIN fornito via SMS all'atto dell'attivazione, piuttosto che un codice OTP inviato per SMS ovvero per e-mail, istallando un'App sul cellulare del genitore/adulto di riferimento e su quello del minore. La sua funzionalità *basic* (ossia il filtro di domini non consentiti) deve essere offerta gratuitamente in maniera non abbinata agli altri *bundle*.

43 https://i2.res.24o.it/pdf2010/S24/Documenti/2024/02/21/AllegatiPDF/7470.pdf
44 *Ibidem*.

L'art. 13 bis co. II^ del Decreto Caivano ha previsto espressamente come – proprio valutando la possibilità che i minori possano indicare delle generalità non corrispondenti a quelle reali al fine di accedere ad "App", piuttosto che ad altre piattaforme esistenti, così venendo in contatto con contenuti altamente nocivi oltre che illeciti – i gestori dei siti web (*latu sensu*) debbano preventivamente verificare la maggiore età dei propri utenti. Inoltre, l'AGCOM – entro 60 gg dall'entrata in vigore del Decreto Caivano – deve aver stabilito, con proprio provvedimento, le modalità tecniche e di processo per l'accertamento della maggiore età[45].

Proprio in attuazione dell'art. 13 bis co. II^ e III^ D. Caivano, l'AGCOM – con delibera del 08 aprile 2025 n. 96 pubblicata in data 12 maggio 2025 – ha dovuto implementare i sistemi di verifica dell'*age verification* attraverso l'attuazione di modalità tecniche e di processo che siano in linea con la normativa surrichiamata proprio per evitare che i minori siano esposti a contenuti che potrebbero nuocere al loro sviluppo fisico, mentale o morale[46].

Anzi, viene anche specificato come esse siano «altamente raccomandate, in quanto efficaci, idonee, proporzionali e funzionali, per il loro stesso utilizzo anche da parte di altri soggetti rispetto a quelli qui direttamente regolati e con riferimento a ulteriori tipologie di contenuti, oltre a quelli a carattere pornografico, che potrebbero comunque nuocere allo sviluppo fisico, mentale o morale dei minori»[47].

Così, a partire dal 12 novembre 2025, i menzionati soggetti che diffondono in Italia immagini e video a carattere pornografico, a prescindere dal paese di stabilimento, sono tenuti a verificare la maggiore età degli utenti, assicurando

45 Art. 13 bis co. 2: «Fermo restando quanto previsto dall'articolo 42 del decreto legislativo 8 novembre 2021, n. 208, i gestori di siti web e i fornitori delle piattaforme di condivisione video, che diffondono in Italia immagini e video a carattere pornografico, sono tenuti a verificare la maggiore età degli utenti, al fine di evitare l'accesso a contenuti pornografici da parte di minori degli anni diciotto. L'Autorità per le garanzie nelle comunicazioni stabilisce, entro sessanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, con proprio provvedimento, sentito il Garante per la protezione dei dati personali, le modalità tecniche e di processo che i soggetti di cui al comma 2 sono tenuti ad adottare per l'accertamento della maggiore età degli utenti, assicurando un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo».

46 https://www.agcom.it/sites/default/files/provvedimenti/delibera/2025/delibera%2096-25-CONS.pdf

47 *Ibidem*.

un livello di sicurezza adeguato al rischio e il rispetto della minimizzazione dei dati personali raccolti in ragione dello scopo[48].

4. *La Legge del 23 settembre 2025 n. 132: il nuovo art. 612 quater cp*

Alla luce di quanto *ut supra* evidenziato, appare evidente la *ratio* che ha spinto il Legislatore a recepire in una specifica normativa il Regolamento UE 2024/1689, proprio a tutela di tutti coloro i quali accedono al mondo dell'A.I., «sia per motivi di ricerca che di sviluppo, di sperimentazione che di innovazione», laddove l'accesso deve sempre avvenire «nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del Diritto dell'Unione Europea e dei principi di trasparenza, di proporzionalità, di sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità» (Art. 3 co. I).

Rimandando al Regolamento UE 2024/1689 per le definizioni tecniche di "sistemi di A.I., modelli di A.I.[49]", è bene precisare come la Legge 132 esplicitamente prevede (anche per i "dati"[50]) che l'utilizzo dei sistemi e modelli di A.I. avvenga senza pregiudizio alla libertà del dibattito democratico (art. 3 co. 4), senza pregiudizio alle libertà di comunicazione, di espressione e di informazione (art. 4 co. 1); ponendo la cybersicurezza come pre-condizione essenziale lungo tutto il ciclo di vita dei sistemi e dei modelli di A.I (art. 3 co. 6), garantendo il diritto di pieno accesso nel rispetto del principio di uguaglianza e di non discriminazione delle persone con disabilità (art. 3 co. 7). Inoltre, specificamente alla tutela dei minori e dei soggetti parimenti vulnerabili, la Legge rafforza il valore «del consenso di chi esercita la responsabilità genitoriale» per

48 Per un maggiore approfondimento, si invita il lettore a collegarsi al link https://www.agcom.it/competenze/consumatori/interventi-regolamentari-tutela-degli-utenti-finali-attuazione-del-nuovo/tutela-minori-age-verification ed alla relativa Lista AGCOM dei soggetti ex art. 13-bis del Decreto Caivano e delibera n. 96/25/CONS.

49 Art. 3 punto 63 - Regolamento (UE): anche laddove tale modello di I.A. sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, a eccezione dei modelli di I.A. utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato.

50 Art. 2 co. I lett. b) Legge 132/2025: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva.

il minore di anni quattordici che accede alle tecnologie di A.I. e il conseguente trattamento relativo ai dati personali dello stesso (art. 4 co. 4) e altre previsioni in specifici ambiti, imponendo un controllo ferreo da parte dell'AgID (Agenzia per l'Italia Digitale) e l'ACN (Agenzia per la cybersicurezza Nazionale), così evidenziando l'importanza che si è voluto (e dovuto) attribuire all'A.I. per l'impatto che la stessa ha sulla nostra quotidianità.

Ebbene, in considerazione degli specifici aspetti esaminati nel presente contributo, una prima analisi della Legge 132 può essere interessante per i *nova* introdotti al Codice penale (art. 26) con l'introduzione di un'ulteriore circostanza aggravante generale e di una nuova fattispecie tipica. In particolare, l'art. 61 n. 11-decies c.p. recita: «l'aver commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o privata difesa, ovvero aggravato le conseguenze del reato»; mentre l'art. 612-quater cp. prevede: «Chiunque cagiona un danno ingiusto a una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è commesso con altro delitto per il quale si procede d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate».

Orbene, nel primo caso, la fattispecie tipica si aggrava proprio attraverso l'uso insidioso dei sistemi di A.I. che, generando "nuovi contenuti" attraverso la rete neurale, può influenzare ambienti fisici o virtuali, così rendendo ancor più difficile l'individuazione, *ab origine*, della condotta delittuosa ovvero aggravando le conseguenze del reato. Nel caso, invece, della fattispecie derubricata come «Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale», si fa riferimento – come anticipato in premessa – ai reati cibernetici. La fattispecie ex-art. 612-quater cp.p. rientra nei c.d. reati comuni poiché può essere realizzata da *chiunque* ed è a condotta vincolata, poiché la norma elenca le modalità con cui si deve realizzare la condotta tipica: cessione, pubblicazione o diffusione di immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di A.I.

Ulteriori elementi caratteristici della condotta sono: l'assenza del consenso della persona malcapitata, l'idoneità della condotta a «indurre in inganno sulla genuinità», il danno ovvero il pregiudizio cagionato di ordine personale, economico, familiare, reputazionale ecc. Si ricorda, opportunamente, che l'induzione in inganno si deve realizzare proprio attraverso l'uso degli *high-tech*

con cui si sono manipolati ovvero falsificati quelle immagini, video o voci così alla perfezione, tali da farli credere reali.

Ebbene, una delle possibili manifestazioni della condotta tipica esaminata può essere il c.d. *Deep nude* ovverosia l'alterazione, a contenuto esplicitamente sessuale, di foto, immagini video così da ledere l'armonico e ordinario sviluppo psico-fisico del minore attraverso l'uso di sistemi di A.I. Foto, video o immagini sono recuperati proprio dai *canali social* in cui il minore pubblica in forma aperta piuttosto che privata i propri dati personali e sensibili senza rendersi conto che quelle piattaforme costituiscono uno dei terreni fertili di recupero di materiale per il *face o body swap* piuttosto che l'*undressing.* Esistono in rete, infatti, numerosi siti che consentono gratuitamente di "modificare" (*swap*) il volto e il corpo di un'immagine così alterandola; così come esistono piattaforme per "svestire/denudare" le immagini presenti su una foto, in modo da ottenere risultati sempre più creativi, innovativi e personalizzati[51]; il potere dell'A.I. nel manipolare le immagini diventa sempre più pregnante e pericoloso specie se usato da mani inesperte, giovani piuttosto che malintenzionate.

La normativa del *parental control* piuttosto che dell'*age verification* è pensata proprio per evitare che i minori di quattordici anni possano iscriversi anzitempo ai canali social e essere, così, esposti anche a siffatti pericoli, ciò non significando che il minore ultra quattordicenne non meriti parimenti tutela, giacché – come sopra evidenziato – il genitore deve tutelare la fragilità e l'insicurezza del proprio figlio da un uso eccessivo del Web ed essere in grado di filtrare, anzitempo, un uso improprio ovvero distorto dello stesso attraverso l'A.I. Occorre che il minore abbia ben chiari i pericoli del Web poiché quella "popolarità" piuttosto che i *likes* non solo possono creare dipendenza, ma determinano pericoli esponenziali anche a causa del carattere di a-spazialità e a-temporalità tipica del cyberspazio, connotato da un forte anonimato[52]. Non esistono confini materiali né temporali, né persone né relazioni reali: la pervasività che connota il Web può essere uno dei fattori di incremento del disagio giovanile piuttosto che di disturbi psicologici o di nuove dipendenze.

Interessante il Rapporto ISTISAN 23-25[53], pubblicato a dicembre 2023, secondo cui

> […] i giovani sono stati definiti "Face down generation" perché sempre chini su un dispositivo digitale, nati e cresciuti in un mondo dove tutto è accessibile

51 https://anakin.ai/de/blog/top-15-undressing-ai-tools-you-should-use-in-2025-it/

52 https://www.salvisjuribus.it/brevi-considerazioni-sulla-natura-e-sulle-caratteristiche-dello-spazio-cibernetico/

53 https://www.iss.it/documents/20126/9340234/23-25+web.pdf/7c107806-50db-5601-c73e-c90badec3765?t=1711719753324

> attraverso la rete, dal cibo ai vestiti, dal gioco agli amici, perfino la scuola [...] presentano fattori di rischio [...] e condizioni di comorbidità possono sviluppare un disturbo [...] rischiando di passare a un uso patologico […] Vi sono fenomeni emergenti come i *challenge*, doxing, sexting e morphing legati all'uso problematico dei *social media* [...].

In effetti, proprio recuperando lo studio di queste e altre dipendenze patologiche derivanti dall'uso di Internet, lo stesso Ministro Valditara, in una nota del 16 giugno 2025, ha ritenuto necessario, in ambito scolastico, «rafforzare le azioni finalizzate a educare all'uso responsabile e consapevole dello smartphone e degli altri strumenti digitali...dedicando notevole attenzione alle tematiche connesse alla diffusione dell'Intelligenza Artificiale [...]»[54]. Queste ed altre tematiche correlate possono essere oggetto di ulteriore approfondimento da parte della comunità scientifica, ricordando che il presente contributo non può ritenersi esaustivo. A ogni conto, restiamo in attesa di avere, nelle aule giudiziarie, le prime applicazioni della normativa in tema di utilizzo dei sistemi di A.I.

54 Circolare Ministeriale n. 3392 del 16 giugno 2025, firmata dal Ministro dell'Istruzione e del Merito, Giuseppe Valditara, entrata in vigore dal 1° settembre 2025.