

L' "EMANCIPAZIONE DIGITALE" DEL MINORE E L'USO INCONSAPEVOLE DELL'AI: L'EFFICACIA DEL QUADRO NORMATIVO E GLI EFFETTI SULLA VALIDITÀ DEL CONTRATTO*

| 483

Di Arianna Alpini

SOMMARIO: 1. La condizione del minore nell'ambiente digitale: "vulnerabilità naturale" e "vulnerabilità artificiale". - 2. Il continuum esistenziale tra online e offline e la cd. maggiore età digitale del minore. - 3. Il quadro normativo di riferimento per la tutela del minore nell'ambiente digitale tra sinergie di protezione e tensioni applicative. - 4. La visione «antropocentrica» della legge italiana sull'AI (l. 132/2025). - 5. L'uso inconsapevole dell'AI da parte del minore e del genitore. - 6. Frammentazione delle soglie anagrafiche per l'accesso dei minori ai servizi digitali. - 7. Verso una "emancipazione digitale". - 8. L'efficacia del quadro normativo: la verifica tecnica dell'età. - 9. L'evoluzione della governance digitale dell'Unione Europea: il pacchetto "Digital omnibus". - 10. Invalidità del consenso per mancanza di consapevolezza: effetti sul contratto. - 11. La consapevolezza del rischio nell'uso dell'AI come principio italo-europeo. - 12. Considerazioni conclusive.

ABSTRACT. Il saggio esamina le dinamiche evolutive della condizione del minore all'interno dell'infosfera digitale, ponendo l'accento sulla transizione dalla vulnerabilità naturale a quella artificiale indotta da algoritmi persuasivi e sistemi di intelligenza artificiale. Attraverso un'analisi del quadro regolatorio multilivello, l'indagine evidenzia le incoerenze derivanti dalla frammentazione delle soglie anagrafiche per l'accesso ai servizi digitali. L'indagine si concentra sugli effetti della manipolazione comportamentale algoritmica sul processo di formazione della volontà del minore e dei genitori, proponendo un ripensamento dei rimedi civilistici tradizionali. Viene teorizzata l'introduzione dell'istituto dell'emancipazione digitale, ispirato all'art. 390 c.c., volto a modulare la capacità d'agire del minore attraverso percorsi di alfabetizzazione e l'assistenza di un curatore digitale (genitore con adeguata formazione) per gli atti a impatto permanente e irreversibile.

The essay examines the evolutionary dynamics of minors within the digital infosphere, emphasizing the transition from natural vulnerability to artificial vulnerability induced by persuasive algorithms and artificial intelligence systems. Through an analysis of the multilevel regulatory framework, the investigation highlights the inconsistencies deriving from the fragmentation of age thresholds for access to digital services. The study focuses on the effects of algorithmic behavioral manipulation on the decision-making process of both minors and parents, proposing a rethinking of traditional civil law remedies. It theorizes the introduction of 'digital emancipation', inspired by article 390 of the Italian Civil Code, aimed at modulating the minor's legal capacity to act through digital literacy programs and the assistance of a digital curator (a properly trained parent) for acts with permanent and irreversible impacts.

L' "emancipazione digitale" del minore e l'uso inconsapevole dell'AI: l'efficacia del quadro normativo e gli effetti sulla validità del contratto (Arianna Alpini)



1. La condizione del minore nell'ambiente digitale: “vulnerabilità naturale” e “vulnerabilità artificiale”.

La tutela dei minori nell'ambiente digitale richiede un salto di paradigma che, accanto alla gestione del rischio tecnico, elabori una riflessione sulla natura stessa dell'individuo e del suo abitare il mondo come *essere in continuo divenire*¹. L'indagine verte sul legame tra vulnerabilità e ambiente, per mostrare che la transizione verso la cosiddetta infosfera² è non un semplice mutamento di scenario, ma il ritrovamento dei confini dell'umanità³.

La vulnerabilità è certamente una condizione ontologica dell'essere umano, al punto da sostituire il mito del “soggetto autonomo e razionale” con quello del “soggetto vulnerabile”⁴, intrinsecamente dipendente dalle relazioni e dalle infrastrutture che ne sostengono l'esistenza⁵.

* Il saggio è la rielaborazione approfondita della relazione tenutasi in occasione del Seminario organizzato dal Prof. A. Gorgoni svoltosi presso il Dipartimento di Scienze Giuridiche dell'Università degli Studi di Firenze il 3 dicembre 2025 dal titolo “*La condizione del minore nell'ambiente digitale: rischi, soluzioni e rimedi*”.

¹ Due sono i contributi della cultura giuridica che hanno impresso in modo indelebile le coordinate dell'evoluzione del concetto di capacità di agire: A. FALZEA, *Il soggetto nel sistema dei fenomeni giuridici*, Milano, 1939, 155 ss. e P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Camerino-Napoli, 1972, 137 ss.

² Il primo utilizzo documentato della parola “infosfera” è rintracciabile in un articolo di R.Z. Sheppard su Time Magazine del 12 aprile 1971 reperibile su: rewriters.it/infosfera-ed-esistenze-onlife, ora vedi L. FLORIDI, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009. Sull'attribuzione di capacità normativa ai poteri diffusi nell'infosfera attraverso le regole tecniche delle piattaforme, v. A. FEDERICO, *Il nomos della 'infosfera'*, in *Rass. dir. civ.*, 2022, 533 ss.; per una rilettura della cultura giuridica digitale come «valore aggiunto strumentale» v. A. GORASSINI, *Il valore della cultura giuridica nell'era digitale*, in *Tecn. dir.*, 2021, 38 ss.

³ Sul tema vedi le chiare pagine di G. VETTORI, *Persona e pluralismo*, Firenze, spec. XIV ss. e 121 ss. Gli studi sull'AI sono proliferati e continuano a sviluppare in modo veloce e incontrollabile ma non altrettanto può dirsi per lo studio da parte del giurista dell'essere umano. Tuttavia, proprio l'evoluzione tecnologica ha fatto emergere la centralità e le peculiarità dell'essere umano, nonché l'esigenza di assegnare una rilevanza giuridica sempre maggiore alla consapevolezza e al processo motivazionale nell'ambito dell'autonomia negoziale: A. ALPINI, *Interpretazione e fonti del diritto tra tradizione e innovazione*, in *Interpretazione e fonti del diritto tra tradizione e innovazione*, in EAD., T. FEBBRAJO e B. MARUCCI (a cura di), Napoli, 2023, 287; EAD., *Il diritto come “arte sociale”. Contributo per una didattica innovativa*, in *Ars interpretandi*, 2025, 2, 53 ss.

⁴ Su questi profili, già N. ZORZI GALGANO, *Il consumatore medio ed il consumatore vulnerabile nel diritto comunitario*, in *Contr. Impr. Europa*, 2010, 549 ss., nonché, per una valorizzazione del contraente debole come persona, L. MEZZASOMA, *Consumatore e Costituzione*, in *Rass. dir. civ.*, 2015, 311 ss. Oggi anche la Corte di Giustizia UE non crede più all'*homo economicus*, razionale ed accorto, poiché la razionalità è limitata dalle distorsioni cognitive: CGUE, 14.11.2024, c. 646-22, in *Foro it.*, 2025 III, 147 ss. con commento di G. BOVA CRISPINO, *L'apertura della Corte di Giustizia ad una interpretazione evolutiva della nozione di consumatore medio: verso un consolidamento della cultura, sul piano giuridico, della “razionalità limitata” a beneficio della libertà di scelta del consumatore*. Vedi S. PAGLIANTINI, *In memoriam del consumatore medio*, in *Eur. dir. priv.*, 2021, 2 ss. Il tema, se pur da diverse angolazioni, è stato indagato anche da: E. NAPOLITANO, *Digital marketing: processi decisionali e relazioni consumeristiche* (77 ss.); P. BENEVEVE, *Neuromarketing, processi decisionali e bias cognitivi* (95 ss.); T. FEBBRAJO, *Influencer marketing e pratiche*

Se la vulnerabilità è il tratto comune ad ogni essere umano in quanto bisognoso di cura e fisicamente finito, tuttavia la vulnerabilità “artificiale” – ovvero quella creata dall’uomo – sottopone l’individuo ad una nuova condizione di precarietà che si potrebbe declinare nella versione economica, sociale e politica: basti pensare all’istituzione di una disciplina dedicata alla tutela del consumatore.

Sopra a tutte le vulnerabilità vi è quella digitale⁶.

In contesti naturali, un dato rimane fisso: l’essere umano ha percezione del tempo e del luogo e dunque di se stesso. L’esperienza umana è situata attraverso il corpo quale “veicolo dell’essere al mondo”⁷, per cui la vulnerabilità è protetta da confini spaziali e temporali abbastanza chiari.

Questa struttura protettiva collassa nell’ambiente *onlife*, in cui la barriera tra analogico e virtuale cade e lo spazio si trasforma in un’infosfera dove il concetto di “distanza” svanisce, poiché tutto è ugualmente vicino e ugualmente lontano⁸.

L’ambiente digitale costituisce terreno fertile per il funzionamento di un’infrastruttura di *business* che vuole modificare il mondo per adeguarlo agli algoritmi di consumo, anche a scapito della complessità umana. In tale contesto, la vulnerabilità del minore costituisce un elemento funzionale a modelli di *business* basati sull’*engagement* compulsivo. Sì che quella che nelle piattaforme appare come socialità o partecipazione è in realtà uno spazio privato che assolve a funzioni pubbliche solo per “trattenere” il consumatore e massimizzare il profitto⁹.

L’algoritmo non è neutrale¹⁰, ma è un atto etico e politico che modella l’autonomia del soggetto attraverso segnali di *engagement* impliciti.

commerciali scorrette (113 ss.), tutti in A. ALPINI, T. FEBBRAJO e B. MARUCCI (a cura di), *op. cit.*

⁵ Sui rapporti tra autonomia e vulnerabilità si rinvia all’approfondimento filosofico di B. PASTORE, *Semantica della vulnerabilità, soggetto e cultura giuridica*, Torino, 2021, *passim*.

⁶ Sulla vulnerabilità nel contesto digitale, che permea l’intera esperienza dell’individuo in rete, v. G. CARAPEZZA FIGLIA, *Vulnerabilità digitale e post-modernità giuridica*, in *Dir. merc. amm. fin.*, 2025, 1 ss.; V. RICCIUTO, *La persona e la vulnerabilità tecnologica: il diritto della tecnologia sostenibile*, in *Riv. dir. impr.*, 2023, 487 ss.

⁷ M. MERLEAU-PONTY, *Phénoménologie de la perception*, Paris, Gallimard, 1945, trad. A. BONOMI, *Fenomenologia della percezione*, Milano, 1965, *passim*.

⁸ L. FLORIDI, *Pensare l’Infosfera. la filosofia come design concettuale*, Milano, 2020, *passim*. Sulla dissoluzione delle dimensioni di spazio e tempo nell’era digitale v. G. PASCUCCHI, *Il diritto nell’era digitale*, Bologna, 2010, 179 ss.; N. IRTI, *L’ordine giuridico del mercato*, Roma-Bari 2009, 150, rileva che «lo spazio telematico è sciolto dalla fisicità: non tanto sta oltre i confini territoriali, quanto non ha confini [...] il tempo non è più storia, ma nella “assolutezza della momentaneità” [...] criterio di calcolo quantitativo».

⁹ G. VETTORI, *Persona e pluralismo*, Firenze, 2024, XVII, il quale descrive in profondità l’aspetto più opaco dell’uso dell’innovazione tecnologica offrendolo alla nostra meditazione: «Le nostre emozioni, carpite dall’espressione del volto, dalle parole, dal movimento degli occhi, sono raccolte e si forma un inconscio digitale, non ancora nostro»; sul problema del consenso nel mondo digitale, vedi 49 ss.

¹⁰ Testualmente, P. ZELLINI, *La dittatura del calcolo*, Milano, 2018, 87, secondo il quale «l’algoritmo non è neutrale e soggetto al nostro arbitrio, ma portatore autonomo di una credibilità che sconfina, a tratti, in una veridicità di stampo divino»; P. PERLINGIERI, *Relazione conclusiva*, in P. PERLINGIERI, S. GIOVA e I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, 2020, 379 ss.; ID., *Diritto civile e Intelligenza Artifi-*



Il minore rappresenta il vertice di questa tensione: la sua vulnerabilità è non solo giuridica, ma neurocognitiva, prodotta da architetture progettate per creare dipendenza, come l'*infinite scroll*¹¹. I dati recenti evidenziano che questa vulnerabilità diventa solitudine, poiché la maggior parte dei minori adolescenti cerca nell'AI un supporto emotivo che non trova più nell'ambiente relazionale fisico¹². L'uso di supplenza della tecnica segnala il fallimento sia dell'ambiente digitale come luogo di autentica crescita sociale, sia della funzione educativa e della formazione culturale.

2. Il continuum esistenziale tra online e offline e la cd. maggiore età digitale del minore.

Il punto di partenza per costruire una tutela effettiva del minore è acquisire la consapevolezza che la società tecnologica espone *tutti* gli individui a un crescente "rischio sistemico", per il quale la vulnerabilità diventa una condizione strutturale¹³. Il minore parte da una situazione che è "oltre la vulnerabilità", essendo sprovvisto della piena *capacitas iudicandi* e dunque più esposto ai rischi derivanti dall'uso precoce e non consapevole degli strumenti digitali.

L'ambiente digitale non è una sfera separata della vita, ma rappresenta l'interazione più assorbente dell'agire umano, dove la relazione con l'AI è intrinsecamente dinamica e conflittuale.

La prima avvertenza metodologica è evitare che la creazione di categorie giuridiche speciali (minore digitale, capacità digitale) ostacoli la valutazione complessiva e unitaria della situazione esistenziale del minore. È necessario mantenere un *continuum* tra la dimensione *offline* e quella *online* quali parti che si compenetrano e che devono essere interpretate l'una attraverso l'altra. Da questa prospettiva, appare ingenuo ritenere che l'ambiente digitale è parte del quadro educativo, considerato che le piattaforme sono mercati per la raccolta di dati strutturati con meccanismi manipolatori che compromettono addirittura l'efficacia del ruolo educativo genitoriale.

Il minore non è "digitale", il minore è un essere umano in divenire al quale va garantito un libero e pieno sviluppo.

La seconda avvertenza riguarda la cd. maggiore età digitale.

ciale, in *Tecn. dir.*, 2025, 135 ss. Vedi, altresì, E. CATERINI, Artificial Intelligence, *persona e soggetto*, in *Tecn. dir.*, 2022, 207 ss.

¹¹ P. PERLINGERI, *Note sul «potenziamento cognitivo»*, in *Tecn. dir.*, 2021, 209 ss.

¹² Vedi in *orizzontescuola.it*. Cfr. le storiche sentenze rispettivamente del 24.3. 2026 State of New Mexico v. Meta Platform, Inc., e del 25.3.2026 K.G.M. v. Meta Platform, Inc., et al. (case No J CCP 5255) in base alle quali si è statuito che le aziende tecnologiche possono essere ritenute responsabili se il design del loro prodotto è intrinsecamente volto a creare comportamenti compulsivi che portano a depressione e ideazione suicida.

¹³ Sul delicato tema: N. LIPARI, *Vulnerabilità esistenziale e strumenti di tutela*, in *Annali Sisdic*, 2018, 2, 4 ss.; A. GORGONI, *La vulnerabilità nell'ambiente digitale e la protezione della libertà del volere*, in *Pers. Merc.*, 2024, 3, 915 ss.

Accanto alla riconosciuta capacità di discernimento del minore¹⁴, si pone la sua speciale vulnerabilità nell'ambiente digitale che riporta l'attenzione sulla fragilità dell'essere umano ancora sprovvisto della piena *capacitas iudicandi*¹⁵.

La consapevolezza, da un lato che la preclusione del compimento di un atto o dell'attività patrimoniale al minore dotato di un sufficiente livello di maturità si tradurrebbe in ostacolo all'esercizio di diritti e libertà fondamentali, e dall'altro della progressiva commistione tra sfera esistenziale e patrimoniale, nonché dell'esistenza di pericolose ed occulte insidie dell'ambiente digitale, impone di affrontare con estrema prudenza il tema della cd. maggiore età digitale¹⁶.

3. Il quadro normativo di riferimento per la tutela del minore nell'ambiente digitale tra sinergie di protezione e tensioni applicative.

La tutela del minore nell'ambiente digitale¹⁷ si articola su una stratificazione composita, costruita essenzialmente su una terna di regolamenti europei (GDPR, DSA, AI Act)¹⁸ che si applicano e si integrano con il diritto nazionale, tra cui in particolare la legge 132/2025. Si aggiungono le direttive dell'Autorità per le Garanzie nelle Comunicazioni-AGCOM, specialmente la Delibera 96/25/CONS¹⁹, volta a dettagliare le misure tecniche e operative necessarie per l'applicazione effettiva dei principi, stabilendo livelli di protezione rigorosissimi che superano gli *standard* tecnici di base dell'Unione. In questo quadro, già piuttosto complesso, vanno inserite anche le Linee

¹⁴ R. SENIGAGLIA, *Minore d'età e contratto. Contributo alla teoria della capacità*, Torino, 2020, *infra*.

¹⁵ Su questi profili, I. GARACI, *Il "superiore interesse del minore" nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in *Nuove leggi civ. comm.*, 2021, 4, 800 ss.

¹⁶ Sulle tensioni fra autonomia progressiva e clausola del *best interest of the child* vedi G. CARAPEZZA FIGLIA, *Autonomia progressiva e costituzionalizzazione del diritto dell'infanzia e dell'adolescenza*, in *Dir. fam. pers.*, 2025, 2, 603 ss.; V. BARBA, *Autonomia progressiva e miglior interesse della persona minore di età*, in *Dir. succ. fam.*, 2023, 441 ss.; G. RECINTO, *Genitori e figli tra tendenze interne «adultocentriche» e spinte apparentemente «minorecentriche» della Corte EDU*, in F. DELL'ANNA MISURALE e F.G. VITERBO (a cura di), *Nuove sfide del diritto di famiglia. Il ruolo dell'interprete*, Napoli, 2018, 75 ss. Sui rischi delle nuove tecnologie per i minorenni sempre nella prospettiva della capacità del minore: S. ORLANDO, *I lividi dei minorenni sparring partners di chatgpt e l'età minima per attivare il servizio in Italia*, in *Pers. merc.* 2023, 1, 3 ss.

¹⁷ Sulla quale si veda l'analisi di E. ADAMO, *Minore età e nuove tecnologie*, Napoli, 2025, *passim*.

¹⁸ In realtà è stata disegnata una architettura della regolazione del digitale in cui ciascuno dei tasselli costitutivi è complementare agli altri (DSA, DMA, DGA, Data Act e AI Act): vedi A. MORACE PINELLI, *Data Act (reg. UE 2023/2854): la circolazione dei dati nell'interesse privato e generale*, in *Nuova giur. civ. comm.*, 2025, 1, 220 ss.

¹⁹ Delibera 96/25/CONS dell'8 aprile 2025, recante "Adozione delle modalità tecniche e di processo per l'accertamento della maggiore età degli utenti in attuazione della legge 13 novembre 2023, n. 159", disponibile su <https://www.agcom.it/provvedimenti/delibera-96-25-cons>.



guida che assumono efficacia “quasi regolamentare”²⁰, essendo richiamate dai regolamenti alle quali rinviano per la concretizzazione dei principi²¹.

Tale materiale normativo ha creato da un lato sinergie di protezione (come nel caso delle Autorità), dall'altro significative tensioni applicative: ne costituisce un esempio paradigmatico il *Digital Omnibus Package* presentato dalla Commissione europea, volto ad armonizzare e coordinare il *corpus* normativo digitale dell'Unione, rafforzando la certezza giuridica e semplificandone l'attuazione, recentemente approvato limitatamente alla proposta di semplificazione dell'*AI Act (Digital Omnibus on AI)*²².

La proposta genera preoccupazione poiché la spinta alla uniformità, implicando necessariamente la centralizzazione e la semplificazione, può tradursi in un indebolimento delle tutele introdotte a livello nazionale, svilendo gli standard elevati imposti da AGCOM, come l'obbligo di segregazione dei dati di *Age Assurance* per scopi non commerciali.

Una delle novità prospettate è la revisione della definizione di “dato personale” prevista nell'art. 4 del GDPR. Secondo la proposta un'informazione non sarebbe considerata dato personale se l'entità che la detiene non dispone di mezzi «ragionevolmente probabili» per identificare l'individuo. Questa versione, che si spinge oltre quanto stabilito dalla giurisprudenza della Corte di Giustizia dell'Unione Europea²³, potrebbe creare scappatoie per i *data*

²⁰ Sul fenomeno del dinamismo e della non ufficialità delle fonti del diritto contemporaneo, vedi P. PERLINGIERI, *Per un positivismo giuridico «inclusivo»*. Note minime su diritto e cultura, in *Annali Sisdic*, 2023, 10, 159 ss.

²¹ A. GORGONI, *Le Linee guida della Commissione europea emanate ai sensi dell'art. 28 DSA: privacy, autonomia e protezione del minore*, in *Corti fiorentine*, 2025, 1-3, 29 ss. ID., *Protezione, educazione e recupero del minore che agisce nello spazio digitale*, in *Pers. merc.*, 2025, 4, spec. 1176 ss. dove l'A. con grande sensibilità pone l'impellente problema di impartire ai minori l'educazione adeguata per acquisire la capacità di valutare criticamente l'affidabilità delle fonti di dati, informazioni e contenuti digitali. Sull'esigenza di una adeguata “preparazione digitale” dei genitori e sulla collaborazione fra tutti i soggetti coinvolti nella formazione del minore, vedi R. SENIGAGLIA, *Dimensione onlife, famiglia e “incapacità dei genitori” di assolvere ai loro compiti*, in *Pers. succ. fam.*, 2025, 2, 511 ss.

²² Il *Digital Omnibus Package* è l'iniziativa di semplificazione della legislazione digitale presentata dalla Commissione europea il 19 novembre 2025, articolata nelle proposte COM(2025) 836 final (*Digital Omnibus on AI*) e COM(2025) 837 final (*Digital Omnibus Regulation*), nonché nelle ulteriori iniziative contestualmente presentate nell'ambito del *Digital Package*. La documentazione ufficiale è disponibile sul portale della Commissione europea: <https://digital-strategy.ec.europa.eu/en/news/simpler-eu-digital-rules-and-new-digital-wallets-save-billions-businesses-and-boost-innovation>. Vedi altresì: EDPB-EDPS *Joint opinion* 2026, 1 del 20.1.2026 on the “Proposal for a Regulation as regards the simplification of the implementation of harmonised rules on artificial intelligence” (*Digital Omnibus on AI*), disponibile in https://www.edpb.europa.eu/documents/legislative-opinion/edpb-edps-joint-opinion-12026-on-the-proposal-for-a-regulation-as_en; EDPB-EDPS *Joint opinion* 2026, 2, dell'11.2.2026 on the “Proposal for a Regulation as regards the simplification of the digital legislative framework” (*Digital Omnibus*), in https://www.edpb.europa.eu/documents/legislative-opinion/edpb-edps-joint-opinion-22026-on-the-proposal-for-a-regulation-as_en. Mentre la procedura legislativa relativa al *Digital Omnibus on AI* (2025/0359 (COD)) può considerarsi sostanzialmente conclusa (Sul punto, *infra*, nota 52), risultano tuttora pendenti sia la procedura 2025/0360 (COD), relativa alla proposta COM(2025) 837 final (*Digital Omnibus Regulation*), sia la procedura 2025/0358 (COD), concernente la proposta COM(2025) 838 final (*European Business Wallets*).

²³ Nelle sentenze relative ai casi Scania (C-319/22) e Single Resolution Board (C-413/23), la Corte di Giustizia aveva suggerito che un'informazione pseudonimizzata, trasmessa da

broker e l'industria pubblicitaria, risultando particolarmente dannosa per i minori.

In un contesto dove i dati vengono costantemente aggregati e incrociati, la tesi per cui un'azienda possa trattare dati pseudonimizzati come se fossero non personali solo perché non ha l'intento immediato di re-identificare l'utente, indebolisce le tutele contro la profilazione invisibile. La protezione del minore deve, invece, essere garantita a prescindere dall'infrastruttura tecnologica del momento, basandosi sulla potenzialità intrinseca dei dati di influenzare il comportamento e lo sviluppo psicofisico dell'essere in divenire.

D'altra parte il Parlamento Europeo ha adottato una risoluzione sulla tutela dei minori *online*²⁴. Questo documento, pur non essendo immediata-

un'entità A a un'entità B, potesse essere qualificata come dato personale per l'entità A anche se quest'ultima non aveva alcun mezzo ragionevole per identificare l'interessato, purché l'entità B (il destinatario) possedesse le chiavi di decodifica o informazioni aggiuntive per l'identificazione. Questa interpretazione "oggettiva" o "assoluta" del dato personale ha generato confusione e incertezza legale, poiché imponeva obblighi di conformità GDPR gravosi anche a soggetti che gestivano dati tecnicamente anonimi dal loro punto di vista. Il nuovo *Digital Omnibus Regulation* interviene direttamente sull'articolo 4, paragrafo 1, del GDPR per sancire legislativamente un "approccio relativo". Vedi in <https://iapp.org/news/a/eu-digital-omnibus-what-the-proposed-changes-to-the-concept-of-personal-data-mean-in-practice>. Sul punto le riflessioni di E. STRINGHI, *Il pacchetto "Digital Omnibus": la proposta della Commissione europea COM(2025) 837 final del 19.11.2025 di modifica del GDPR, del Data Act, del regolamento sullo sportello unico digitale e delle direttive e-privacy, NIS2 e CER, nonché di abrogazione della direttiva Open Data, del Data Governance Act, del regolamento P2B e del regolamento sulla libera circolazione dei dati non personali*, in *Oss. Pers. Merc.*, 2025, 3, 1033 ss.; EAD., *Il parere congiunto EDPB-EDPS n. 2/2026 del 10.2.2026 sulla proposta Digital Omnibus COM(837) riguardante la semplificazione del quadro della legislazione digitale*, *ivi*, 2026, 1, 278 ss., dove l'A., prendendo in esame il *Joint Opinion* EDPB-EDPS 2/2026, cit., evidenzia che la modifica proposta rischia di restringere la nozione di dato personale e l'ambito applicativo del GDPR, trascurando elementi centrali del concetto di identificabilità, quali il *singling out*, e creando margini per possibili aggiramenti della disciplina, con conseguente indebolimento delle garanzie poste a tutela dei diritti e delle libertà fondamentali degli interessati.

²⁴Il primo passo significativo del Parlamento europeo è stato l'adozione della risoluzione del 12 dicembre 2023 sul *design* additivo dei servizi *online* e la tutela dei consumatori (2023/2043(INI)).

La risoluzione ha evidenziato che le direttive esistenti, quali la Direttiva sulle pratiche commerciali sleali (2005/29/CE) e la Direttiva sui diritti dei consumatori (2011/83/UE), pur essendo efficaci nel proteggere gli interessi economici tradizionali, manchino di definizioni legali precise per affrontare la manipolazione comportamentale mediata dagli algoritmi. Il Parlamento ha, dunque, esortato la Commissione europea a introdurre il concetto di "diritto a non essere disturbati" e a stabilire standard di "*ethical design by default*". Tra le raccomandazioni chiave del 2023 figurano: la proibizione delle tecniche più dannose di *design* additivo che sfruttano le vulnerabilità cognitive, l'obbligo di disattivare per impostazione predefinita le funzionalità di coinvolgimento estremo; la garanzia di trasparenza sui sistemi di raccomandazione, permettendo agli utenti di scegliere feed non basati sulla profilazione. Sulla qualificazione dell'*addictive design* come «pratica commerciale scorretta», v. F. ESPOSITO e T. MACIEL CATHOUD FERREIRA, *Addictive Design as an Unfair Commercial Practice: The Case of Hyper-Engaging Dark Patterns*, in *Eur. Journ. Risk Regulation*, 2024; 15(4), 999-1016.

Il 26 novembre 2025, il Parlamento europeo ha adottato una nuova risoluzione 2025/2060(INI) specificamente dedicata alla protezione dei minori *online*. Il fulcro della risoluzione è la proposta di stabilire un limite di età digitale armonizzato a livello



mente vincolante, stabilisce le priorità del legislatore europeo per contrastare i fenomeni di dipendenza digitale e i rischi della manipolazione algoritmica. Il Parlamento ha espresso la necessità di superare la frammentazione delle soglie anagrafiche, proponendo un limite digitale europeo armonizzato a 16 anni per l'accesso ai social media, alle piattaforme video e ai compagni virtuali basati su AI (*AI companions*).

Al di sotto di tale soglia, l'accesso dovrebbe essere consentito solo con il consenso documentato dei genitori. Inoltre, il Parlamento ha fissato a 13 anni il limite assoluto sotto il quale nessun minore dovrebbe poter accedere ai *social media*, indipendentemente dal consenso genitoriale.

Il consenso, sebbene necessario, non è considerato uno strumento sufficiente a mitigare i rischi intrinseci di piattaforme progettate per massimizzare il tempo di permanenza dell'utente attraverso l'uso di tecnologie persuasive²⁵. La Risoluzione individua specifiche funzionalità tecnologiche che devono essere proibite o disabilitate di *default* per i minorenni, in quanto configurano una vera e propria «progettazione della dipendenza» (*Addiction by Design*), quali ad esempio lo scorrimento infinito (*Infinite Scroll*), meccanismo che elimina i punti di interruzione naturale della navigazione, favorendo il consumo compulsivo di contenuti; la riproduzione automatica (*Autoplay*), funzionalità che spinge l'utente verso una visione passiva e ininterrotta; algoritmi basati sull'*Engagement*, ovvero sistemi di raccomandazione che assumono come prioritari contenuti iper-personalizzati e volti a mantenere alta l'attenzione, spesso a scapito del benessere mentale; meccanismi di gioco d'azzardo (*Loot Boxes*)²⁶, cioè funzionalità presenti nei videogiochi che incentivano la spesa economica basata sulla casualità, sfruttando la mancanza di alfabetizzazione commerciale dei bambini.

4. La visione «antropocentrica» della legge italiana sull'AI (l. 132/2025).

dell'Unione Europea. Il Parlamento chiede che l'età minima predefinita per l'accesso ai social media, alle piattaforme di *video-sharing* e ai compagni virtuali basati su AI sia fissata a 16 anni. Sul fenomeno del cd. *sharenting*, si rinvia a G. CARAPEZZA FIGLIA, *Effettività della tutela del minore e misure di coercizione indiretta. Gli artt. 614-bis e 709-ter c.p.c. nella riforma del processo della famiglia*, in *Dir. fam. pers.*, 2022, 2, 640 ss.; I. GARACI, *La responsabilità genitoriale nella complessità dell'ecosistema digitale. Riflessioni alla luce della legge n. 132/2025 sull'intelligenza artificiale*, in *Dir. Internet*, 2026, 1, 43; N. MATTA, *Sharenting e tutela della persona minore di età*, in *Tecn. dir.*, 2022, 285 ss. In prospettiva comparata, si veda lo studio di G. SANTONI, *La tutela dei minorenni verso le piattaforme online: prospettive di diritto comparato*, in *Ann. dir. comp.*, 2023, 443 ss.

²⁵ Sui limiti dell'efficacia del consenso, v. A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, 82 ss.; più in generale, sul ruolo del consenso nel sistema della protezione dei dati, R. CATALANO, A. ESPOSITO e R. PICARO (a cura di), *Il diritto alla protezione dei dati personali. Profili evolutivi della giurisprudenza e della dottrina*, Napoli, 2025, spec. 11 ss. Riguardo alla tutela dei minori nell'ambiente digitale, v. l'analisi di D. MARCELLO, *Circolazione dei dati del minore tra autonomia e controllo. Norme e prassi nel mercato digitale europeo*, Napoli, 2023, spec. 73 ss.

²⁶ Sul tema si veda: M. PERINI (a cura di), *Il gioco d'azzardo: una prospettiva multidisciplinare. Atti del convegno tenutosi presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Siena il 1° dicembre 2023*, Firenze, 2024, *passim*.

L'elemento distintivo e fondante della legge italiana sull'AI (l. 132/2025)²⁷ è la sua esplicita adozione di una "visione antropocentrica" (art. 1, Finalità e ambito di applicazione)²⁸. Questa clausola generale di salvaguardia dell'umano informa tutte le successive disposizioni di trasparenza, responsabilità, equità e rispetto dei diritti fondamentali.

L'antropocentrismo è volto ad assicurare che il progresso tecnologico sia guidato e limitato dalla priorità della persona e che l'essere umano mantenga il controllo sui processi decisionali. Tale visione è tradotta in specifici obblighi che garantiscono che la responsabilità e la supervisione nell'utilizzo dei sistemi di AI rimangano saldamente ancorate all'individuo.

La declinazione più sensibile e innovativa della visione antropocentrica si ritrova nell'art. 4 che disciplina specificamente la tutela dei soggetti minorrenni nell'utilizzo dei sistemi di Intelligenza Artificiale. L'ordinamento italiano stabilisce che l'età minima per il consenso autonomo al trattamento dei propri dati personali (inclusa la profilazione) è di 14 anni, definendo di fatto una "maggiore età digitale"²⁹. Nel caso in cui il minore non abbia raggiunto tale soglia, il trattamento è lecito solo se e nella misura in cui il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale. Il titolare del trattamento è tenuto a compiere "sforzi ragionevoli" per verificare che tale consenso sia effettivamente dato o autorizzato.

La genericità della locuzione "sforzi ragionevoli" ha portato i fornitori di servizi a ricorrere a metodi inefficaci, come la mera autodichiarazione dell'età. Per questo, la legge 132/2025, pur riaffermando che il minore che ha compiuto i 14 anni può esprimere il proprio consenso per il trattamento dei dati personali connessi all'utilizzo di sistemi di intelligenza artificiale, rafforza questa soglia di consenso. Il legislatore riconosce implicitamente che i rischi derivanti dall'opacità algoritmica e dalla profilazione ad alta intensità superano la portata della "ragionevolezza" richiesta dal GDPR per il consenso generale³⁰. Di conseguenza, si introduce un *obbligo informativo*

²⁷ Per un commento al testo legislativo, si rinvia, per tutti a R. D'ANGIOLELLA, *Legge 23 settembre 2025, n. 132. La tutela della persona nella regolazione dell'intelligenza artificiale*, Napoli, 2025, *passim*.

²⁸ Sulla ambiguità della prospettiva antropocentrica: A. ALPINI, *Sull'approccio umano-centrico all'intelligenza artificiale. Riflessioni a margine del "Progetto europeo di orientamenti etici per una IA affidabile"*, in *comparazionedirittocivile.it* (aprile 2019) e EAD. *Digital divide, censura digitale e antropocentrismo dei dati*, *ivi*, 2021, 879 ss. Più in generale, sul tema, v. S. LABATE, *Umanismi senza antropocentrismo. Note sul post-human*, in *Filosofia e teologia*, 2015, 1, 72 ss.

²⁹ Vedi art. 8 Reg. 2016/679 (GDPR) e art. 2 *quiquies* d.lg. 196/2003 (Codice Privacy).

³⁰ Con l'avvento dei *social networks* (C. PERLINGIERI, *Profili civilistici dei social networks*, Napoli, 2014) e dei sistemi di AI, il legislatore ha dovuto prendere atto dell'insufficienza di un modello basato esclusivamente sul consenso spesso rilasciato in modo meccanico e sotto il peso di asimmetrie informative insuperabili [S. ORLANDO (a cura di), *Libertà e liceità del consenso nel trattamento dei dati personali*, in *personaemercato.it*, 2, 2024]. Il GDPR ha introdotto il principio di *accountability* e obblighi di trasparenza più stringenti (sui quali M. D'AMBROSIO, *Accountability e tutela dell'Utente*, in *Corti salernitane*, 2024, 1, 3 ss.) mentre l'*AI Act* ha adottato un approccio basato sul rischio, categorizzando i sistemi in base al loro potenziale impatto sui diritti fondamentali (cfr. M. R. NUCCIO, *Intelligenza Artificiale (IA) e gestione dei rischi: prospettive di tutela*, in *Rass. dir. civ.*, 2022, 4, 1466 ss.). In questo contesto, l'informativa diventa strumento di bilanciamento del potere contrattuale l'assenza della quale mina la possibilità stessa dell'accordo.



rinforzato: le comunicazioni relative al trattamento dei dati connesse all'utilizzo di sistemi di intelligenza artificiale devono essere rese con linguaggio chiaro e semplice, in modo da risultare facilmente accessibili e comprensibili ai minori.

Il requisito linguistico, che a prima vista appare meramente formale, asurge invece a condizione essenziale per garantire la trasparenza epistemica e l'effettivo esercizio del controllo.

Il principio emergente, ovvero quello della cd. riserva di umanità³¹ è il filo conduttore della legge italiana che si dipana nell'obbligo della spiegabilità in capo agli utilizzatori dei sistemi di AI - che implica conoscibilità del funzionamento, trasparenza e tracciabilità dell'utilizzo -, (art. 3 comma 3), e nella tutela del diritto di autore per le opere generate con l'assistenza dell'AI, a condizione che l'opera costituisca il risultato del lavoro intellettuale dell'autore ovvero dell'«ingegno umano» (art. 25)³².

L'informativa richiesta a tutela dei minori deve garantire all'utente la conoscibilità dei relativi rischi e il diritto di opporsi ai trattamenti autorizzati dei propri dati personali. Tale approccio eleva il requisito formale di consenso a un requisito sostanziale di consapevolezza del rischio, rendendo la validità del consenso (anche a 14 anni) dipendente dalla qualità e comprensibilità dell'informativa e non solo dall'età anagrafica.

5. L'uso inconsapevole dell'AI da parte del minore e del genitore.

³¹ J. VALERO TORRIJOS, *Les garanties juridiques de la intel·ligència artificial en l'activitat administrativa des de la perspectiva de la bona administració*, in *Revista Catalana De Dret Públic*, 2019, 58, 82-96, ha introdotto il concetto di riserva d'umanità. La genesi della riflessione è strettamente legata a casi giudiziari di rilievo in Spagna, come la controversia relativa al cosiddetto Bono Social, un sussidio elettrico per famiglie vulnerabili gestito attraverso l'algoritmo BOSCO. In tale contesto, la Fundación Ciudadana Civio impugnò il diniego di accesso al codice sorgente dell'algoritmo, portando alla luce le criticità dell'opacità decisionale. Valero Torrijos individuò nella riserva di umanità lo strumento per garantire che l'automazione non si traducesse in una delegittimazione delle procedure democratiche. Per lo studioso spagnolo, la riserva d'umanità non è un divieto assoluto di automazione, bensì l'obbligo di mantenere un intervento umano significativo capace di controllare, validare o smentire la decisione automatizzata. In Italia, il concetto di riserva d'umanità ha trovato la sua massima espressione e sistematizzazione dogmatica nell'opera di G. GALLONE, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Padova, 2023, sottolinea che la riserva d'umanità è un limite ontologico: sebbene la tecnologia possa aumentare l'efficienza, non può sostituire l'imputabilità della scelta autoritativa. Gallone rintraccia la ragion d'essere di questo principio nel timore che il genere umano possa rendere superfluo sé stesso, delegando la gestione della *polis* ad agenti artificiali privi di responsabilità democratica.

³² G. FINOCCHIARO, *La legge italiana in materia di intelligenza artificiale. Una prima lettura*, in G. CERRINA FERRONI, S. ORLANDO e G. VETTORI (a cura di), *Il regolamento europeo sull'intelligenza artificiale. Problemi e sistema*, Bologna, 2026, 353 ss. Sul disegno di legge oggetto del dibattito parlamentare, v. anche la proposta della Società Italiana degli Studiosi del Diritto Civile (S.I.S.Di.C.), Commissione di studio in tema di Intelligenza artificiale, D.d.l. n. 1146 - Disposizioni e delega al Governo in materia di intelligenza artificiale, in *Ann. SISDiC*, 2025, 83 ss. Si veda altresì, A. ALPINI, *Artificial intelligence e creazione artistica*, in *Tec. Dir.*, 2024, 1, 1 ss.

L'utilizzo di sistemi di intelligenza artificiale spesso implica la gestione di processi complessi (come l'addestramento di modelli di AI o l'analisi predittiva) che generano rischi difficili da percepire anche per un utente adulto. Sì che la legge sull'AI impone l'obbligo di rendere tali rischi palesi con la conseguenza che se l'informativa presentata è redatta in linguaggio giuridico-burocratico, tecnico-algoritmico, o è strutturalmente oscura, il consenso espresso dal minore – sebbene legalmente capace – è da considerarsi non valido e il trattamento illecito.

Questo requisito spinge i titolari ad implementare un vero e proprio approccio di *privacy by design* linguistica e interattiva³³. Ciò comporta la necessità di integrare l'informativa nell'interfaccia utente (UX/UI) con elementi che ne facilitino la fruizione (come infografiche o icone) e che siano adattati al livello di maturità cognitiva media della fascia 14-18 anni.

L'onere di dimostrare l'adempimento dell'obbligo di linguaggio chiaro e semplice ricade sul titolare del trattamento in virtù del principio di *accountability* stabilito dal GDPR. L'art. 7, paragrafo 1 stabilisce che, se il trattamento si basa sul consenso, il titolare deve essere in grado di dimostrare che l'interessato lo ha prestato. Tale onere si estende oltre la mera prova formale dell'ottenimento del consenso (il *click* di accettazione) per includere la prova della sua qualità.

Il fornitore del sistema AI è il soggetto su cui grava l'onere di dimostrare che, per gli utenti minorenni (dai 14 anni in su), le informazioni e le comunicazioni sono state redatte con linguaggio particolarmente chiaro e semplice, facilmente accessibile e comprensibile dal minore. La legge italiana innalza il livello di dettaglio richiesto per questa prova, poiché non è sufficiente dimostrare "cosa" è stato comunicato, ma è necessario dimostrare "come" è stato comunicato e se la metodologia adottata fosse oggettivamente adeguata al *target* minorenne.

Dimostrare la chiarezza e la semplicità del linguaggio in modo oggettivo richiede l'adozione di rigorosi strumenti di documentazione e audit interni. Di conseguenza i DPO dovranno integrare nei loro processi di *Privacy Impact Assessment* (PIA) un'analisi specifica sulla "Comprensibilità Linguistica per i servizi AI". Gli elementi essenziali per soddisfare l'onere della prova includeranno la prova documentale dell'uso di tecniche di presentazione adeguate, come la struttura a livelli (informazioni stratificate), l'uso di elementi multimediali (video, infografiche) e la scelta di caratteri e spaziature che migliorino la leggibilità e l'accessibilità. Infine, sarà necessario il mantenimento di un registro dettagliato (ai sensi dell'art. 30 GDPR) di tutte le versioni delle informative e della documentazione di supporto, per dimostrare che la specifica informativa presentata al minore al momento dell'espressione del consenso sia conforme allo *standard* della legge³⁴.

³³ Su tale nozione, v. A. CAVOUKIAN, S. TAYLOR e M.E. ABRAMS, *Privacy by Design: essential for organizational accountability and strong business practices*, in *Identity in the Information Society*, 2010, 3, 405- 413. Cfr. L. GATT e D. BORELLI, *Privacy by Design and by Default and Data Protection Impact Assessment (DPIA)*, in *Eur. Journ. Privacy Law & Techn.*, 2019, 1, 100 ss.

³⁴ Sui rapporti tra valutazione d'impatto, tutela dei diritti fondamentali e *accountability*, v. P. PASQUALONE, *Impact Assessments and the Protection of Fundamental Rights in the Processing of Personal Data*, in *It. Law Journ.*, 2025, 2, 441 ss.



La l. 132/2025 stabilisce una chiara inversione della presunzione in tema di *compliance*, poiché in assenza di prova documentale della chiarezza oggettiva, si presume che il fornitore abbia violato la legge. L'obbligo probatorio così rafforzato implica che il Garante Privacy può utilizzare la mancata dimostrazione di un linguaggio oggettivamente chiaro e misurabile come strumento primario per contestare l'illiceità del trattamento in caso di indagine. La sanzione può derivare non solo dall'aver trattato dati in modo non trasparente, ma dal non aver documentato che il linguaggio fosse conforme allo *standard* elevato richiesto per il minore, rappresentando una violazione di *accountability* aggravata dal *target* vulnerabile.

Il mancato adempimento della prescrizione rafforzata di chiarezza invalida il fondamento stesso del trattamento. Di conseguenza, l'attività di trattamento dei dati personali del minore da parte del sistema AI risulta illecita per violazione diretta dei principi cardine del GDPR, in particolare dei principi di trasparenza, liceità e *accountability* (art. 5 GDPR).

La ricaduta sul contratto della non conformità del trattamento alle indicate prescrizioni del GDPR può ben essere ricondotta alla nullità di protezione *ex artt. 36 e 135-octies* cod. cons.³⁵.

Tuttavia, occorre chiedersi se tale rimedio sia coerente con il quadro delineato a tutela del minore, come integrato dalla legge italiana che, rafforzando la prescrizione di chiarezza e comprensibilità, sembra consolidare e valorizzare il passaggio dal «consenso» alla «consapevolezza» quale principio italo-europeo direttamente incidente nella disciplina del contratto.

Inoltre, posto che l'obbligo di rendere l'informativa chiara e comprensibile in modo che il consenso sia consapevole *ex artt. 3 e 4* legge 132/2025, si estende anche al genitore che presta il consenso per il figlio, occorre chiedersi se, ove mancasse il consenso del genitore per l'accesso del minore di anni 14, l'annullabilità prevista dall'art. 1425 c.c. risulterebbe il rimedio più adeguato.

6. Frammentazione delle soglie anagrafiche per l'accesso dei minori ai servizi digitali.

La tutela dei minori è un asse portante del DSA, il quale prescrive, in particolare, il divieto completo di pubblicità mirata, riconoscendo che la vulnerabilità cognitiva del minore rende il consenso (anche se genitoriale) uno strumento insufficiente³⁶.

³⁵ Vedi A. MORACE PINELLI, *op. cit.*, 227-228; S. PAGLIANTINI, *L'attuazione minimalista della Direttiva 2019/770/UE: riflessioni sugli artt. 135 octies - 135 vicies ter c.cons.*, in *Nuove leg. civ. comm.*, 2022, 149 ss.; ID., *Un giro d'orizzonte sulle nullità del terzo millennio*, in *Studi senesi*, 2020, 295 ss. e in *Persona e mercato*, 2021, 31 ss; S. POLIDORI, *Nullità di protezione e sistematica delle invalidità negoziali*, Napoli, 2016, *passim*.

³⁶ L'innovazione più dirompente del DSA (Reg. UE 2022/2065) in materia di tutela dell'infanzia è contenuta nell' art. 28, paragrafo 2, che proibisce esplicitamente ai fornitori di piattaforme *online* di presentare pubblicità basata sulla profilazione quando sono consapevoli, con ragionevole certezza, che il destinatario del servizio è un minore. In generale, sul tema, v. G. SPOTO, *Disciplina del consenso e tutela del minore*, in S. SICA, V.

Le piattaforme accessibili ai minori (*ex art. 28 DSA*) sono obbligate ad adottare misure adeguate, tra cui la necessità di modificare i sistemi di raccomandazione per ridurre la probabilità che i minori entrino in contatto con contenuti dannosi. Specifiche raccomandazioni tecniche indirizzano le piattaforme a dare priorità ai segnali espliciti forniti dai minori (come le impostazioni dirette) rispetto ai segnali comportamentali (profilazione implicita). Inoltre, le linee guida per l'attuazione dell'art. 28 del DSA (che richiede "misure adeguate e proporzionate") impongono di disabilitare di default le funzionalità di progettazione più avvincenti (*Addiction by Design*), come lo scorrimento infinito, la riproduzione automatica e le *push notifications*.

Per le piattaforme di dimensioni molto grandi (VLOP), il DSA impone l'obbligo di analizzare e mitigare i "rischi sistemici". L'art. 34, par. 1, lettera d), cita come categoria di rischio la manipolazione intenzionale del servizio con effetti negativi sulla tutela della salute pubblica e dei minori e le gravi conseguenze negative per il benessere fisico e mentale della persona³⁷.

L'intervento normativo va oltre la mera gestione dei contenuti illegali, riconoscendo esplicitamente il *danno alla salute mentale e psicofisica* derivante dall'uso eccessivo della piattaforma, elevando così la progettazione dell'interfaccia a un requisito di *compliance* legale³⁸. Si intende impedire che la mancanza di alfabetizzazione commerciale dei bambini sia sfruttata, proteggendoli da pratiche che possono portare a spese indesiderate o comportamenti di dipendenza, come l'uso di *loot box* o determinate valute virtuali.

In questo contesto, la Proposta di Legge n. 1136 (DDL 1136)³⁹ rappresenta un significativo intervento che si concentra sull'accesso ai servizi di *social media* e sulla regolamentazione dei *baby influencer*. Un elemento centrale è la disciplina della validità dei contratti per i servizi della società dell'informazione ad alto rischio. L'art. 3 stabilisce che i contratti relativi ad *account* creati e detenuti da minori di età non superiore a 15 anni sono da

D'ANTONIO e G.M. RICCIO, (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 111 ss.

³⁷ Il riconoscimento del danno alla salute è diventato centrale nelle recenti azioni di controllo della Commissione Europea. Ad esempio, nel procedimento contro TikTok, l'accusa preliminare riguarda proprio la violazione del DSA attraverso un *design* studiato per creare dipendenza (scorrimento infinito, notifiche *push* costanti), che ignorerebbe i rischi per la salute fisica e mentale dei minori, influenzando negativamente il loro sviluppo cognitivo. In tema, v. F. GALLI, *La pubblicità mirata al tempo dell'intelligenza artificiale: quali regole a tutela dei consumatori*, in *Contr. e impr.*, 2022, 3, 919 ss.; S. M. LENER, *Piattaforme, inferenze e profilazione. Il quadro normativo della pubblicità mirata alla luce della giurisprudenza della Corte di Giustizia dell'UE*, in *Analisi Giuridica dell'Economia*, 2025, 1, 129 ss.

³⁸ Il Considerando 81 stabilisce esplicitamente che le piattaforme devono valutare se i minori possano imbattersi in contenuti che possano nuocere alla loro salute o al loro sviluppo fisico, mentale e morale. Specifica, inoltre, che i rischi possono derivare dalla progettazione di interfacce che sfruttano l'inesperienza dei minori o causano comportamenti di dipendenza. Il considerando 83 si focalizza sui rischi derivanti dalla progettazione del servizio (come il design additivo), riconoscendo che tecniche volte a massimizzare l'ingaggio possono avere effetti negativi sulla salute mentale e causare un uso compulsivo. Vedi sul tema, A. GORGONI, *Protezione, educazione e recupero del minore nello spazio digitale*, in *Pers. merc.*, 2025, 4, 1151 ss.

³⁹ DDL S. 1136, recante "Disposizioni per la tutela dei minori nella dimensione digitale", presentato in data 13 maggio 2024 e attualmente in corso di esame in commissione.



considerarsi nulli in assenza di consenso o autorizzazione del titolare della responsabilità genitoriale. L'innalzamento della soglia di validità contrattuale a 15 anni costituisce un disallineamento rispetto alla soglia di consenso digitale di 14 anni. Con questa misura, il legislatore esprime una valutazione implicita dell'inadeguatezza della *capacitas iudicandi* sotto i 15 anni per la gestione di atti negoziali dal decisivo impatto sull'identità del minore e sul profilo economico, avvicinandosi allo spirito della Risoluzione del Parlamento europeo.

7. Verso una "emancipazione digitale".

Nell'ambiente digitale emerge chiaramente l'inadeguatezza della tradizionale distinzione tra atti di ordinaria e straordinaria amministrazione. Un *post* sui *social* o la condivisione di una immagine possono apparire come atti di ordinaria amministrazione, ma le loro conseguenze in termini di indicizzazione permanente e danno reputazionale li rendono atti di straordinaria amministrazione per i loro effetti irreversibili.

La pluralità di soglie anagrafiche evidenzia altresì la necessità di un modello di capacità elastica e funzionale⁴⁰.

L'utilizzo della capacità di agire come criterio di proporzionalità regolatoria sposta il *focus* dall'essere soggetto di diritto alla facoltà di compiere atti validi, emancipando di fatto il minore⁴¹. Per modulare la capacità di discernimento *on line* del minore senza soffocarne lo sviluppo, si potrebbe rileggere l'istituto della emancipazione in chiave digitale (emancipazione digitale). Tale istituto potrebbe offrire la sponda per garantire l'esercizio in autonomia di specifici diritti, riservandone altri al controllo del genitore.

L'emancipazione digitale, mutuando dall'art. 390 c.c. la logica della capacità assistita, si sgancerebbe dai presupposti matrimoniali per essere condizionata al superamento di percorsi certificati di *digital literacy*⁴². L'obiettivo dell'emancipazione digitale sarebbe consentire l'autonoma gestione degli Atti di Ordinaria Amministrazione Digitale, come l'iscrizione a servizi base, senza il costante coinvolgimento genitoriale. Il Curatore Digitale (normalmente il genitore formato) assisterebbe il minore negli Atti di Straordinaria Amministrazione Digitale. Estendendo il concetto di straordi-

⁴⁰ R. SENIGAGLIA, *Minore d'età e contratto*, cit., spec., 54 ss.; G. CARAPEZZA FIGLIA, *Teoria della capacità e tutela della persona umana. Per una nuova dogmatica minorile*, in *Rass. dir. civ.*, 2024, 325 ss.: sulla scia di P. PERLINGIERI, *Sui rapporti personali nella famiglia*, in *Dir. fam. pers.*, 1979, 1253 ss. ora in ID., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, 2005, 467 ss. vedi anche P. STANZIONE, *Potestà dei genitori e diritti fondamentali del minore*, in *Rass. dir. civ.*, 1980, 446 ss.

⁴¹ Sul superamento della rigida ed omologante concezione degli incapaci e su una nozione relativa di capacità: P. PERLINGIERI, *La personalità umana*, cit., 137 ss. Su questa scia: P. STANZIONE, *Capacità e minore età nella problematica della persona umana*, Camerino-Napoli, 1975. Sull'autonomia del minore necessaria per poter svolgere la sua personalità: M.C. BIANCA, *Diritto civile*, I, *La norma giuridica*, I, *I soggetti*, Milano, 1978, 214 ss.

⁴² Sul valore della *digital literacy* quale percorso di formazione all'esercizio consapevole, critico ed eticamente responsabile della cittadinanza digitale, C. COSTA, e M. OLIVER, *Young people and digital literacy learning: co-producing critical citizenship practices*, in *Pedagogy, Culture & Society*, 2025, 1-20.

naria amministrazione oltre la sfera patrimoniale, includendo il rischio reputazionale e quello allo sviluppo sano e libero della personalità, si supera l'incompatibilità dello schema classico con l'ambiente digitale.

Da questa prospettiva si configurano come di straordinaria amministrazione tutti gli atti (ma non soltanto quelli) che creano: un impatto irreversibile sull'identità digitale; la compromissione del diritto all'oblio ed effetti permanenti sulla personalità; la *datafication* massiva e non necessaria; il conferimento di dati in eccesso rispetto alle finalità del servizio; la generazione di rilevanti introiti economici; l'impiego commerciale del minore (*baby influencer*) oltre specifiche soglie.

In questi casi, l'intervento del giudice tutelare diventerebbe residuale, limitato a conflitti di interessi o rischi psico-sociali gravi. Parimenti, il genitore vedrebbe recuperato il suo ruolo di responsabile dell'educazione e della formazione del figlio, perché l'emancipazione offre un addentellato per compensare la sottrazione di competenza che il riconoscimento dell'autonomia del consenso a 14 anni di fatto implica. Tale riconoscimento di autonomia comporta, infatti, la cessazione dei sistemi di controllo parentale, ma al contempo il mantenimento della responsabilità oggettiva dei genitori per il danno cagionato da fatto illecito del minore, con una prova liberatoria che, in questo contesto, risulta quasi impraticabile⁴³.

La modulazione della capacità secondo una gradualità progressivamente emancipatoria calibrata sugli atti lascerebbe al genitore una funzione di assistenza sino ai 18 anni di età del figlio. Questa visione trasformerebbe il ruolo del genitore da *controllore* a *facilitatore* dello sviluppo digitale, in linea con quanto raccomandato dall'Autorità garante per l'Infanzia in merito alla necessità di promuovere percorsi di *digital literacy* per l'intero nucleo familiare⁴⁴, riallineando la responsabilità genitoriale alla corrispondente funzione educativa.

8. L'efficacia del quadro normativo: la verifica tecnica dell'età.

L'efficacia del quadro normativo dipende in gran parte dalla capacità tecnica dei titolari del trattamento di verificare l'età⁴⁵.

La Delibera AGCOM n. 96/25/CONS stabilisce un quadro tecnico rigoroso per l'accertamento della maggiore età degli utenti (*Age Assurance*), in

⁴³ Sul punto, G. CARAPEZZA FIGLIA, N. CIPRIANI, G. FREZZA, G. PERLINGIERI, P. VIRGADAMO e I. ZINGALES, *Illeciti e rimedi civili nei rapporti familiari*, in ID., *Manuale di diritto di famiglia*, Napoli, 2^a ed., Napoli, 2024, 285 ss. Sul contenuto e l'ampiezza dell'onere probatorio, v. Cass., 10.9.2019, n. 22541, in *Resp. civ. prev.* 2020, 2, 505; Cass., 18.11.2014, n. 24475, in *Dir. e Giust.* 19.11.2014.

⁴⁴ A. CORDIANO, *Cyberbullismo e responsabilità civile (ovvero «come abbiamo smesso di vivere il reale»)*, in *Corti fiorentine*, 2025, 1-3, 57 ss. Vedi, sul punto il recente schema di decreto legislativo attuativo della legge italiana sull'AI (132/2025) alle disposizioni del Regolamento UE 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 in materia di poteri delle autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione.

⁴⁵ Sull'analisi degli strumenti esistenti a tale scopo, v. S. TROZZI, *La tutela dei minori nel prisma della protezione dei dati personali. I sistemi di verifica dell'età tra personalismo ed esigenze di bilanciamento fra diritti*, in *Riv. it. inf. dir.*, 2024, 2, 39 ss.



attuazione del “Decreto Caivano” (L. 159/2023). L’obiettivo fondamentale è impedire l’accesso dei minori (soglia di 18 anni) innanzitutto a contenuti a carattere pornografico *online*⁴⁶.

La delibera AGCOM impone che i sistemi di *Age Verification* garantiscano un meccanismo di doppio anonimato volto a risolvere il potenziale conflitto tra la necessità di protezione e il diritto alla riservatezza.

Il doppio anonimato prevede due livelli di segregazione dei dati:

1. Il fornitore del servizio di verifica (*Identity Provider*) non deve sapere a quale specifico sito *web* o piattaforma l’utente sta accedendo.

2. La prova della maggiore età fornita al sito *web* (*Service Provider*) non deve contenere dati identificativi dell’utente.

Inoltre, è richiesto che i dati personali raccolti o generati nell’attuazione degli obblighi relativi alla verifica dell’età non siano trattati per scopi commerciali, come *marketing* diretto, profilazione o pubblicità comportamentale mirata. Tale divieto impone la separazione netta tra i dati di autenticazione dell’età e i dati di *business* intelligence. Il doppio anonimato e la segregazione dei dati creano un muro normativo e tecnico tra le informazioni di identità anagrafica del minore e gli interessi di profitto della piattaforma, impedendo la mercificazione di tali dati sensibili⁴⁷. L’utilizzo di un intermediario indipendente e certificato per la fornitura della “prova della maggiore età” garantisce che questi requisiti di *privacy* siano rispettati.

È emersa, tuttavia, la criticità legata all’uso delle VPN che permettono di aggirare facilmente le restrizioni connettendosi a server esteri non soggetti alla giurisdizione italiana⁴⁸. Per ovviare a questo problema, la Commissione Europea ha iniziato a pilotare una soluzione di verifica dell’età interoperabile a livello UE, basata sul prototipo di un’app di *Age Verification* che è stata testata da Italia, Francia, Spagna, Grecia e Danimarca⁴⁹.

La prospettiva futura è l’integrazione sistematica della verifica dell’età all’interno del portafoglio di identità digitale europeo (*EUDI Wallet*). Questo strumento consentirebbe di scambiare attributi minimi certificati (come

⁴⁶ Delibera 96/25/CONS recante “Adozione delle modalità tecniche e di processo per l’accertamento della maggiore età degli utenti”, in attuazione della legge 13 novembre 2023, n. 159, disponibile su www.agcom.it/provvedimenti/delibera-96-25-cons.

⁴⁷ Sul valore economico dei dati personali e sui rischi connessi alla loro mercificazione nel contesto delle piattaforme digitali, V. RICCIUTO, *Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in *Riv. dir. impr.*, 2021, 261 ss.; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in ID., V. CUFFARO e R. D’ORAZIO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 23 ss.; A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, *ivi*, 1381 ss.; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020.

⁴⁸ Cfr. *Tutela dei minori e verifica dell’età: Agcom adotta i primi ordini di blocco di siti pornografici inadempienti*, in www.agcom.it/comunicazioni/comunicati-stampa.

⁴⁹ Cfr. “Commission makes available an age-verification blueprint”, 14 luglio 2025, notizia disponibile su: <https://digital-strategy.ec.europa.eu/en/news/commission-makes-available-age-verification-blueprint>.

il superamento della soglia dei 18 anni) in modo sicuro e transfrontaliero, riducendo la necessità per le piattaforme di raccogliere dati eccessivi⁵⁰.

A tal proposito, il DDL 1136 italiano prevede che, entro il 30 giugno 2026, sia reso disponibile un mini-portafoglio nazionale per la verifica dell'età degli utenti dei *social network*, anticipando la piena attuazione del sistema europeo⁵¹.

9. L'evoluzione della *governance* digitale dell'Unione Europea: il pacchetto “Digital omnibus”.

L'effettività della tutela dei minori dipende in larga misura dalla evoluzione della *governance* digitale dell'Unione Europea, non sempre coerente con i valori che ne stanno alla base. Il “Digital Omnibus Package”, con l'obiettivo di semplificare il quadro normativo, ridurre gli oneri burocratici e stimolare la competitività tecnologica europea, inaugura una fase di ricalibrazione strutturale che solleva interrogativi profondi sulla tenuta dei diritti fondamentali.

L'intersezione tra le modifiche al Regolamento Generale sulla Protezione dei Dati (GDPR) e alla Legge sui Dati (*Data Act*), contenute nella proposta 837, e i “raffinamenti” alla Legge sull'Intelligenza Artificiale (*AI Act*), introdotti dal *Digital Omnibus on AI*, ormai sostanzialmente approvato⁵², crea un nuovo sistema normativo in cui la tutela del minore finisce per dipendere dalle capacità tecniche dei titolari del trattamento e dalle dinamiche di mercato⁵³.

⁵⁰ Commissione europea, Blueprint for an Age Verification Solution to Help Protect Minors Online, 2025, disponibile su <https://digital-strategy.ec.europa.eu/en/factpages/blueprint-age-verification-solution-help-protect-minors-online>.

⁵¹ DDL S. 1136, recante “Disposizioni per la tutela dei minori nella dimensione digitale”, cit., spec. art. 2 (rubricato “Disposizioni per l'accesso di minori ai servizi di media sociale e alle piattaforme di condivisione di video”), comma 2: «Nelle more dell'adozione di ragionevoli misure tecniche uniformi europee, i fornitori di servizi di *social network online* e di piattaforme di condivisione di video verificano l'età degli utenti mediante un mini-portafoglio nazionale che attua la soluzione dell'Unione europea di verifica dell'età, tenendo conto delle modalità stabilite dall'Autorità per le garanzie nelle comunicazioni. Il mini-portafoglio è reso disponibile entro il 30 giugno 2026».

⁵² Si segnala che, con riferimento al c.d. *Digital Omnibus on AI* (COM(2025) 836 final), a seguito dell'accordo politico provvisorio raggiunto nell'ambito del trilogio tra Parlamento europeo, Consiglio e Commissione europea il 6 maggio 2026, successivamente formalizzato nel documento del Consiglio ST 9247/2026 del 13 maggio 2026 (disponibile all'indirizzo: <https://data.consilium.europa.eu/doc/document/ST-9247-2026-INIT/en/pdf>), il Parlamento europeo ha approvato il testo e il Consiglio ha successivamente adottato l'atto, firmato dai Presidenti delle due istituzioni l'8 luglio 2026 (https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=consil:PE_30_2026_INIT). Alla data di chiusura del presente lavoro, si è in attesa della pubblicazione dell'atto nella Gazzetta ufficiale dell'Unione europea. Di contro, la proposta COM(2025) 837 final concernente la revisione del c.d. *data acquis* è invece tuttora all'esame delle istituzioni europee.

⁵³ I. GARACI, *La responsabilità genitoriale nella complessità dell'ecosistema digitale. Riflessioni alla luce della legge n. 132/2025 sull'intelligenza artificiale*, in *Dir. Internet*, 2026, 1,37 ss.

La modifica più radicale introdotta dalla proposta 837 riguarda l'emendamento dell'art. 4 del GDPR relativo alla definizione di "dato personale". La proposta introduce un approccio "relativo" all'identificabilità, stabilendo che un'informazione non sia necessariamente un dato personale per ogni entità, ma solo per quella che dispone di mezzi "ragionevolmente probabili" per identificare la persona fisica. Questo cambiamento creerebbe una zona d'ombra normativa assai pericolosa: le aziende che operano in ambiti come l'*EdTech* o il *gaming* potrebbero sostenere che i dati raccolti (biometria latente, stili di interazione, preferenze di apprendimento), se trattati in forma pseudonimizzata, non costituiscano dati personali.

La proposta n. 837 stabilisce il "legittimo interesse" come base giuridica per lo sviluppo e l'addestramento di sistemi di intelligenza artificiale. La struttura operativa della norma sposta l'onere della prova dal fornitore all'individuo, passando da un modello di consenso preventivo (*opt-in*) a uno di opposizione (*opt-out*) di difficile gestione per il minore⁵⁴.

La proposta permette, inoltre, il trattamento di dati sensibili "residui" (come l'origine etnica o l'orientamento sessuale presenti nei post sui social media) se la loro rimozione richiederebbe uno "sforzo sproporzionato"⁵⁵. Ciò significa che frammenti dell'identità digitale del minore potrebbero rimanere permanentemente codificati all'interno di modelli di IA, esponendolo a rischi di discriminazione algoritmica a lungo termine senza che i genitori abbiano avuto la possibilità di esprimere un consenso informato.

Una modifica particolarmente discussa riguardava l'art. 4 dell'*AI Act* relativo all'alfabetizzazione sull'IA. La proposta n. 836 della Commissione aveva infatti sostanzialmente sostituito l'originario obbligo gravante su fornitori e *deployer* con un'attività di "incoraggiamento" affidata alla Commissione e agli Stati membri. Il testo successivamente approvato dai colegislatori ha successivamente corretto tale impostazione, reintroducendo un obbligo in capo a fornitori e *deployer*, seppur in forma attenuata: non più quello di garantire un livello sufficiente di *AI literacy*, ma soltanto di adottare misure volte a sostenerne lo sviluppo, precisando ulteriormente che non esiste alcun obbligo di garantire un determinato livello di alfabetizzazione per ogni singolo individuo⁵⁶.

In contesti educativi, dove l'IA viene utilizzata per valutare gli studenti o personalizzare i percorsi didattici, permane il rischio che un obbligo di *AI literacy* meno incisivo o mirato si traduca in una preparazione non uniforme

⁵⁴ Cfr. anche Considerando 31, che menziona il «diritto incondizionato di opporsi al trattamento dei loro dati personali».

⁵⁵ Cfr. Considerando 33 e art. 3 punto 6 della proposta n. 837. L'articolo citato prevede una modifica all'art. 13 del GDPR con l'aggiunta del par. 5.

⁵⁶ Cfr. art. 1 Reg. *Omnibus* digitale sull'IA, punto 5): Articolo 4. Alfabetizzazione in materia di IA: «I fornitori e i *deployer* di sistemi di IA adottano misure volte a sostenere lo sviluppo dell'alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati. Tale obbligo non impone ai fornitori o ai *deployer* di garantire un livello specifico di alfabetizzazione in materia di IA per alcuna persona» (corsivi aggiunti). Il testo in italiano è reperibile su <https://data.council.europa.eu/doc/document/PE-30-2026-INIT/it/pdf>.

del personale scolastico. Ciò potrebbe favorire un affidamento eccessivo a sistemi di IA non pienamente compresi, indebolendo l'effettività della supervisione umana e, indirettamente, lo sviluppo del pensiero critico degli studenti⁵⁷.

Va, invece, valutata positivamente la scelta di non confermare l'esonero dalla registrazione per i fornitori che, pur rientrando nelle categorie sensibili dell'Allegato III (quali l'istruzione), ritengano autonomamente che il proprio sistema non presenti rischi significativi *ex art. 6, par. 3*. Tale modifica era stata inizialmente prospettata dalla proposta n. 836 mediante la soppressione di un inciso dell'art. 6, par. 4, e dell'art. 49, par. 2⁵⁸. Il testo approvato ha, invece, mantenuto l'obbligo di registrazione, limitandosi a semplificare le informazioni da comunicare mediante la modifica della sezione B dell'Allegato VIII (cfr. Considerando 22).

Il mantenimento dell'obbligo di registrazione lascia pertanto invariato il sistema di trasparenza previsto dall'*AI Act* e consente a cittadini, ricercatori, autorità di controllo e società civile di conoscere l'esistenza e l'impiego di sistemi di IA in settori particolarmente sensibili. La permanenza della registrazione nel *database* europeo preserva inoltre importanti forme di tracciabilità e scrutinio esterno, riducendo il rischio che valutazioni effettuate unilateralmente dai fornitori sottraggano tali sistemi a un adeguato controllo pubblico.

Con riferimento alla tempistica applicativa, è stato invece confermato il differimento dell'entrata in vigore degli obblighi per i sistemi ad alto rischio, in seguito alla modifica dell'art. 113 par. 3 lett. c). Di conseguenza, l'applicazione delle norme per i sistemi educativi sarà posticipata fino al 2 dicembre 2027, e per i prodotti come i giocattoli intelligenti fino al 2 agosto 2028⁵⁹.

Il ritardo creerà un vuoto di tutela proprio in una fase di espansione massiccia dell'AI generativa, durante il quale i minori continueranno a interagire con sistemi non certificati che potrebbero mancare dei requisiti minimi di robustezza, accuratezza e supervisione umana. Particolarmente grave è, per l'effetto, il rinvio degli obblighi di trasparenza anche per i contenuti manipolati (*Deepfake*), previsto dall'art. 50(2)⁶⁰ tramite l'introduzione del nuovo par. 4 all'art. 111.

⁵⁷ Tuttavia, lo schema di decreto legislativo attuativo della legge italiana sull'AI (132/2025) alle disposizioni del Regolamento UE 2024/1689 del parlamento europeo e del consiglio del 13 giugno 2024 in materia di poteri delle autorità nazionali e di utilizzo dell'intelligenza artificiale nella formazione prevede nel Capo III disposizioni mostrano una effettiva consapevolezza della emergenza educativa e formativa di studenti, docenti, professionisti, P.A. e adulti.

⁵⁸ Cfr. punti 6) e 14) della proposta originaria della Commissione europea n. 836.

⁵⁹ Cfr. art. 1 Reg. *Omnibus* digitale sull'IA, cit., punto 40 lett. b), Articolo 113, par. 3, lett. c): «il capo III, [...] si applica a decorrere dal: i) 2 dicembre 2027 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 2, e dell'allegato III; e ii) 2 agosto 2028 per quanto riguarda i sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, e dell'allegato IX. (corsivi aggiunti).

⁶⁰ Sebbene si sia anticipato il termine per la conformità nel testo di compromesso, passando dal 2 febbraio 2027 al 2 dicembre 2026. Cfr. art. 1 Reg. *Omnibus* digitale sull'IA, cit., punto 39 lett. b). In un contesto in cui il *cyberbullismo* basato sulla creazione di immagini sessualmente esplicite generate dall'IA è in aumento, posticipare gli strumenti di rilevamento e

La proposta 837 interviene anche sul *Data Act*, restringendo drasticamente le condizioni per l'accesso ai dati da parte del settore pubblico (B2G). Se il quadro originario permette tale accesso in caso di "eccezionale necessità" per compiti di interesse pubblico, la nuova versione, attraverso l'introduzione del nuovo art. 15 *bis*, limita tale possibilità alle sole "emergenze pubbliche" catastrofiche⁶¹.

Limitando l'accesso ai soli casi di emergenza immediata, si perderebbe la capacità di prevenzione e di definizione di politiche basate sull'evidenza per proteggere il benessere psicofisico delle nuove generazioni.

Il *Digital Omnibus* mira a risolvere la cosiddetta "*cookie fatigue*" attraverso eccezioni al consenso per finalità a "basso rischio", come la misurazione dell'*audience*. Tuttavia, la proposta n. 837 permetterebbe un tracciamento continuo all'interno di ecosistemi di siti appartenenti allo stesso proprietario senza che i genitori possano intervenire tramite i *banner* di consenso⁶².

Sebbene i dati non debbano essere condivisi con terzi, le grandi piattaforme possono costruire profili comportamentali estremamente dettagliati dei minori utilizzando queste metriche come base per il proprio *profiling* interno, eludendo la necessità di una scelta attiva. Inoltre, l'esenzione concessa ai "fornitori di servizi mediatici" dall'obbligo di rispettare i segnali automatici di scelta dell'utente costringe i minori a interagire con *banner* complessi, spesso progettati con *dark patterns* per indurre al consenso forzato, ignorando le impostazioni di *privacy* del *browser* o del dispositivo⁶³.

Una ulteriore novità rilevante di COM(2025) 836, confermata anche nel testo adottato, è l'estensione delle agevolazioni previste per le PMI anche alle cosiddette "Small Mid-Caps" (SMC), imprese con meno di 750 dipendenti. Queste aziende potranno fornire documentazione tecnica semplificata e saranno soggette a sanzioni proporzionate alla loro vitalità economica⁶⁴.

marcatura lascia le vittime minorenni prive di strumenti di difesa essenziali. In dottrina si veda: A. CORDIANO, *op. cit.*, 57 ss., ma già EAD., *Cyberbullismo e maleducazione digitale: la legge n. 71 del 2017 tra nuove politiche rieducative e strumenti tradizionali*, in *Foro nap.*, 2021, 41 ss.

⁶¹ Anche l'EDPB e il GEPD, nel *Joint Opinion* 2026, 1, cit., 35, hanno evidenziato alcune criticità della proposta, sottolineando in particolare l'assenza di una motivazione adeguata a sostegno della modifica e la mancata indicazione di esempi concreti nei quali l'accesso a dati personali non pseudonimizzati risulterebbe necessario per rispondere a un'emergenza pubblica in modo tempestivo ed efficace.

⁶² V. Proposta COM(2025) 837, cit., spec. 15, ove si richiama la «stanchezza da consenso»; per il trattamento senza consenso, v. 8: «Le modifiche proposte prevedono inoltre determinate finalità per le quali non dovrebbe essere necessario ottenere il consenso e il successivo trattamento dovrebbe essere considerato lecito, in particolare se presentano un rischio limitato per i diritti e le libertà degli interessati o se l'inserimento di tali tecnologie è necessario per la fornitura di un servizio richiesto dall'interessato», e 17.

⁶³ Vedi C. PERLINGIERI, *Libertà di espressione e di informazione nella comunicazione digitale*, in *Rass. dir. civ.*, 2023, 494 ss.; G. SCOGNAMIGLIO, *Diritto 4.0: criticità, soluzioni e prospettive dell'intelligenza artificiale*, Napoli, 2026, 50 ss.; N. CIPRIANI e G. PERLINGIERI (a cura di), *La tutela dei minori*, in *Le tutele dei minori*, I, diretto da R. Tiscini, Napoli, 2026, 227 ss.

⁶⁴ Cfr. art. 1 Reg. *Omnibus* digitale sull'IA, cit., punto 1 (modifica dell'art. 1(2), lett. g)); punto 10 (modifica dell'art. 11(1)); punto 11 (modifica dell'art. 17(2)); punto 38 (modifica dell'art. 99).

Tuttavia, la dimensione di un'azienda non è un indicatore della pericolosità del sistema di AI prodotto. Un'impresa di medie dimensioni che sviluppa *software* per il monitoraggio biometrico nelle carceri minorili o per l'assegnazione automatica dei voti nelle scuole può causare danni sistemici ai diritti dei minori tanto quanto una *Big Tech*.

Il pacchetto *Omnibus* propone, infine, una centralizzazione della supervisione che sposta l'asse dalle autorità nazionali verso organi dell'Unione. L'*AI Office* della Commissione diventerà l'unico supervisore per i sistemi basati su modelli GPAI e per quelli integrati nelle grandi piattaforme online (VLOP) come *TikTok* o *YouTube*. Parallelamente, l'ENISA svilupperà un "punto di ingresso unico" per la segnalazione di violazioni di dati ai sensi di molteplici regolamenti (GDPR, NIS2, DORA)⁶⁵.

Sebbene la centralizzazione miri a garantire coerenza, si intravede il rischio che le violazioni dei dati dei minori vengano trattate come puri incidenti tecnici di *cybersecurity*, ignorando l'impatto granulare sui diritti umani. Le autorità nazionali per la protezione dei minori o della *privacy* potrebbero ricevere informazioni filtrate o ritardate dall'*AI Office* o dall'ENISA, compromettendo la loro capacità di intervenire tempestivamente a tutela dell'identità digitale dei bambini coinvolti in fughe di dati o manipolazioni algoritmiche⁶⁶.

10. Invalidità del consenso per mancanza di consapevolezza: effetti sul contratto.

Nonostante il panorama normativo delineato sia non soltanto complesso ma anche in continua evoluzione, la legge italiana presenta una carica valoriale che contribuisce significativamente al dibattito sugli effetti dell'invalidità del consenso al trattamento dei dati sul contratto.

Acquisita la natura contrattuale dei rapporti tra piattaforme e utenti⁶⁷, nonché il riconoscimento dell'autonomia progressiva che deve investire an-

⁶⁵ L'ENISA riceve un nuovo ruolo attraverso l'articolo 6 della proposta n. 837, che modifica la direttiva NIS 2 introducendo il nuovo art. 23 *bis* ("Punto di accesso unico per la segnalazione di incidenti"). In base a questa disposizione: «L'ENISA istituisce e mantiene un punto di accesso unico con l'obiettivo di sostenere il rispetto dell'obbligo di segnalare incidenti ed eventi correlati» La Relazione illustrativa spiega poi la *ratio* della misura: «I punti 1) e 2) istituiscono il punto di accesso unico per la segnalazione degli incidenti, includendo obblighi specifici per l'ENISA. È inoltre stabilito che la segnalazione degli incidenti prevista dalla direttiva NIS 2 dovrebbe avvenire attraverso il nuovo punto di accesso unico» (24 ss.).

⁶⁶ Su questi profili, M. FOGLIA, *Identità digitale, trattamento dei dati e tutela della persona*, in *Rass. dir. civ.*, 2021, 80 ss., nonché con specifico riguardo ai minori, E. ADAMO, *L'identità del minorenne nella rete tra istanze di protezione e prospettive rimediali*, in *Dir. fam. pers.*, 2023, 4, 1677 ss.

⁶⁷ P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, 481 ss.; V. RICCIUTO, *L'equivoco della privacy. Persona vs Dato personale*, Napoli, 2022, spec. 139 ss.; R. SENIGAGLIA, *Minore età e contratto*, cit., 117 ss. si veda altresì C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, *passim*; G. CAPILLI, *La tutela dei dati personali dei minori*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*,



che gli atti patrimoniali quando il minore è munito di discernimento (specialmente per contratti identitari o della vita corrente)⁶⁸, occorre fare i conti sia con le specifiche insidie dell'ambiente digitale sia con l'architettura dei rimedi civili nel sistema italo-europeo delle fonti⁶⁹.

La questione riguarda non soltanto la protezione dei dati personali ma investe la tenuta stessa del vincolo contrattuale, ponendo interrogativi sulla qualificazione della patologia negoziale. È chiaro che la soluzione del quesito richiede l'individuazione dell'interesse e dunque il valore da tutelare, atteso che il migliore interesse del minore è soltanto una formula che nulla dice a proposito del rimedio più adeguato da applicare⁷⁰.

Se questo problema era già stato rilevato in dottrina per la tutela del consumatore, in particolare con riferimento al *neuromarketing*⁷¹, nel contesto della tutela del minore e della legge italiana sull'AI, esso presenta profili ancora più delicati e meno esplorati.

Scritti in memoria di S. Rodotà, Milano, 2019, 253; EAD., *Minori in rete tra consenso e verifica dell'età. Analisi comparata e proposte di adeguamento al GDPR*, in *MediaLaws*, 2024, 1, 53 ss.; A. ASTONE, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019, 25 ss.; EAD., *L'accesso dei minori d'età ai servizi della c.d. Società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul Codice per la protezione dei dati personali*, in *Contr. impr.*, 2019, 614 ss.

⁶⁸ R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, cit., 75 ss. V. anche D. DI SABATO, *Le relazioni economiche del minore*, in *Dir. succ. fam.*, 2015, 700 ss.

⁶⁹ A. MANIACI, *Dalle nullità speciali domestiche alle nullità di protezione europee, e ritorno*, in *Pers. merc.*, 2025, 4, 1193 ss.

⁷⁰ P. PERLINGIERI, *Il giusto rimedio nel diritto civile*, in *Giusto proc. civ.*, 2011, 1 ss.; G. PERLINGIERI, *Ordine pubblico e identità culturale. Le Sezioni unite in tema di c.d. maternità surrogata*, in *Dir. succ. fam.*, 2019, 2, Editoriale. L'evoluzione del quadro normativo arricchito dal principio del *best interest of the child* risulta in sintonia con la revisione interpretativa della teoria della capacità nel segno dell'argomento costituzionale: G. CARAPEZZA FIGLIA, *Autonomia progressiva e costituzionalizzazione del diritto dell'infanzia e dell'adolescenza*, in *Dir. fam. pers.*, 2025, 2, 600 ss.; N. CIPRIANI, *The best interest of the child*, in ID. e G. PERLINGIERI (a cura di), *I minori e la famiglia*, in *Le tutele dei minori*, I, diretto da R. Tiscini, Napoli, 2026, 357 ss.

⁷¹ In dottrina sul punto vedi S. ORLANDO (a cura di), *Profili giuridici del neuromarketing. Annuario 2023-2024 OGID Osservatorio Giuridico sull'Innovazione Digitale*, Roma, 2025; B. PARENZO, *"Neuromarketing": un inventario di (spuntati) divieti contro il pericolo di una scelta manipolata*, in *Pers. Merc.*, 2024, 2, 539 ss.; L. TAFARO, *Neuromarketing e tutela del consenso*, Napoli, 2018, 75 ss. e anche A. PANICHELLA, *La tutela del consumatore alla sfida del neuromarketing*, in *Federalismi*, 2024, 6, 223 ss.; ID., *Neuromarketing: ponderazione del consenso e "giusto rimedio" contrattuale*, in *Tecn. dir.*, 2025, 2, 389 ss.; Cfr. D. RUSSO, *Pubblicità ad personam, neuromarketing e tutela del consentire*, in *Tecn. dir.*, 2025, 1, 152 ss. il quale nel contesto dell'indebito condizionamento (vedi artt. 24 e 27 cod. cons.) della pubblicità digitale riserva interessanti considerazioni sugli effetti della manipolazione sul consenso nella prospettiva rimediaria. L'A. rileva condivisibilmente che il vizio del consenso derivato dalla manipolazione del pensiero si colloca spesso più a monte dell'errore, corrispondendo talvolta ad un difetto di ponderazione che può dare luogo a nullità, anche se nei casi più gravi si colloca nella genesi dell'autodeterminazione la quale viene indebitamente indotta. Nella letteratura specialistica di psicologia del lavoro e delle organizzazioni si veda: P. BENEVEVE, *Neuromarketing, processi decisionali e bias cognitivi*, in A. ALPINI, T. FEBBRAJO e B. MARUCCI (a cura di), *op. cit.*, 95 ss.

Per comprendere come l'informativa carente si traduca in una patologia contrattuale è necessario sottolineare il cambiamento di paradigma avvenuto nel passaggio dalla Direttiva 95/46/CE al GDPR, e poi all'*AI Act*.

Per decenni, il consenso è stato interpretato come il pilastro centrale della protezione dei dati, espressione pura della volontà e dell'autonomia decisionale dell'individuo. In tale ottica, l'informativa serviva a garantire l'esercizio del diritto di autodeterminazione, permettendo al soggetto di decidere se e come i propri dati potessero circolare.

Con l'avvento dei *social network* e dei sistemi di intelligenza artificiale, il legislatore ha dovuto prendere atto dell'insufficienza di un modello basato esclusivamente sul consenso, spesso rilasciato in modo automatico o sotto il peso di asimmetrie informative e cognitive insuperabili⁷². Il GDPR ha, quindi, introdotto il principio di *accountability* e obblighi di trasparenza più stringenti, mentre l'*AI Act* ha adottato un approccio basato sul rischio, categorizzando i sistemi di AI in base al loro potenziale impatto sui diritti fondamentali.

In questo contesto, l'informativa diviene uno strumento di bilanciamento del potere contrattuale, l'assenza o incompletezza del quale mina la possibilità stessa di un accordo.

Il GDPR stabilisce che il consenso debba essere libero, specifico, informato e inequivocabile per essere considerato una valida base giuridica del trattamento. L'*AI Act* eleva questo *standard* introducendo il concetto di spiegabilità e trasparenza tecnica per i sistemi ad alto rischio. L'informativa deve coprire non solo le finalità del trattamento dei dati, ma anche la logica di funzionamento dell'algoritmo, i parametri utilizzati e le modalità con cui l'*output* influenza le decisioni che riguardano l'interessato⁷³.

La carenza di tali informazioni determina un "inquinamento" del processo formativo della volontà. Se l'utente non è posto in condizione di comprendere il funzionamento del sistema, il suo consenso non può essere considerato informato, rendendo il trattamento dei dati illecito.

Tuttavia, il problema risiede nel determinare se tale illiceità travolga o no l'intero contratto.

Il GDPR mira a tutelare l'autodeterminazione dell'interessato, considerato la parte "debole" del rapporto. Secondo la previsione dell'art. 7, par. 2 del GDPR, le clausole che violano il regolamento non sono vincolanti, sì che questo si traduce in una nullità parziale che colpisce la singola clausola o il

⁷² C. PERLINGIERI, *Profili civilistici*, cit., 13 ss.; A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1381 ss. Cfr. C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione dei dati personali*, in *Giust. civ.*, 2019, 499 ss.; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, 19 ss.

⁷³ Su questi profili, di recente A. ALPINI e P. SERNANI, *La «spiegabilità algoritmica» e il «danno ermeneutico»*, in *Tecn. Dir.*, 2026, 1, 1 ss. V. anche S. PAGLIANTINI, *"Cognitive sovereignty", diritti digitali e "due process for automated predictions": vizi e virtù di un diritto soggettivo alla spiegazione dell'algoritmo*, in *Foro it.*, 2025, 4, 186 ss; G. CARAPEZZA FIGLIA, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Pers. Merc.*, 2023, 4, 638 ss.



trattamento illecito, ma che, per il principio di conservazione del contratto a favore della parte protetta, non travolge l'intero accordo a meno che non sia il consumatore a richiederlo o sia funzionale al suo interesse.

Tuttavia, se la violazione riguarda norme qualificabili come imperative, in quanto poste a tutela di un interesse di ordine pubblico, può configurarsi la nullità⁷⁴. Del resto, se l'intero oggetto del contratto o la sua causa sono illeciti perché basati su uno scambio di dati ottenuto in modo totalmente coercitivo o manipolatorio (come nelle pratiche vietate dall'*AI Act* richiamate in sinergia con il GDPR), il contratto è nullo *ab origine*, l'azione è imprescrittibile e rilevabile d'ufficio senza limitazioni a favore della parte debole.

Parimenti l'articolo 5 dell'*AI Act* elenca una serie di pratiche di intelligenza artificiale radicalmente vietate nell'Unione Europea poiché contrarie ai valori fondamentali di dignità e libertà. Si tratta di sistemi volti alla manipolazione comportamentale, allo sfruttamento di vulnerabilità psicologiche, al *social scoring* o al riconoscimento delle emozioni sul posto di lavoro. In effetti, in questi casi, la nullità colpisce direttamente la causa e/o l'oggetto del contratto: se la prestazione dedotta in obbligazione consiste in un'attività illecita (come la manipolazione del comportamento tramite AI), l'intero negozio è affetto da nullità assoluta, rilevabile d'ufficio e imprescrittibile⁷⁵.

La mancanza di informativa è assorbita dalla gravità del divieto: anche in presenza di un'informativa completa, il contratto rimarrebbe nullo poiché l'oggetto è sottratto alla disponibilità delle parti. Invece, nel caso in cui il sistema di AI sia lecito ma il fornitore ometta informazioni cruciali prescritte dalla legge, riemerge la figura della nullità di protezione, estesa dalla tutela del consumatore al mercato dei dati e dell'AI, attesa la finalità, anche in questo contesto, di riequilibrare un'asimmetria informativa.

Va precisato che se i requisiti di *data governance* e tracciabilità previsti dall'*AI Act* per i sistemi ad alto rischio (artt. 10 e 12) fossero integrati nelle clausole contrattuali, la violazione di tali obblighi informativi potrebbe essere interpretata come una violazione di norme di protezione, legittimando l'utente a chiedere la nullità delle singole clausole vessatorie o dell'intero contratto se l'opacità del sistema impedisse del tutto la realizzazione dell'interesse contrattuale in modo sicuro e trasparente.

11. La consapevolezza del rischio nell'uso dell'AI come principio italo-europeo.

L'art. 3 della l. 132/2025 stabilisce i principi generali che devono informare la ricerca, la sperimentazione, lo sviluppo, l'adozione e l'applicazione

⁷⁴ G. PERLINGIERI e G. ZARRA, *Ordine pubblico interno e internazionale tra caso concreto e sistema ordinamentale*, Napoli, 2019, spec. 82 ss.

⁷⁵ S. ORLANDO, *Consenso al trattamento e liceità*, in *Pers. merc.*, 2024, 333 ss. Precisa D. RUSSO, *op. cit.*, 161 ss. che, mentre la dimensione dell'indebito condizionamento implica una volontà negoziale riferibile al contraente - dal medesimo maturata in via autonoma se pur suscettibile di condizionamento e di fatto abusivamente influenzata -, le attuali conoscenze della neuroscienza possono addirittura formare il pensiero e la stessa autodeterminazione al compimento dell'atto.

di sistemi e modelli di intelligenza artificiale⁷⁶. Questi principi non sono meri auspici etici, ma costituiscono veri e propri parametri di legalità che condizionano la validità di ogni atto derivato dall'utilizzo di tali tecnologie. La legge prescrive il rispetto rigoroso dei diritti fondamentali e delle libertà previsti dal sistema italo-europeo, ponendo l'accento sulla trasparenza, la proporzionalità, la sicurezza, la protezione dei dati personali e l'accuratezza.

L'obbligo di garantire la sorveglianza e il controllo umani (*human-in-the-loop*) implica che nessuna decisione che abbia impatti significativi sulla persona possa essere delegata interamente a un algoritmo senza una procedura di revisione umana. La violazione di questo principio generale di trasparenza e controllo umano si riverbera direttamente sulla validità del consenso: se il genitore non è informato del fatto che il sistema opera in modo autonomo o non è a conoscenza dei limiti di tale automazione, il suo consenso non può considerarsi "informato" secondo i canoni della *data protection*.

Inoltre, l'utilizzo dei sistemi di intelligenza artificiale non deve recare pregiudizio allo svolgimento con metodo democratico della vita istituzionale e politica, e deve garantire la parità di accesso senza discriminazioni⁷⁷. Anche da questa prospettiva, la protezione dei minori assume una evidente connotazione di ordine pubblico, poiché l'esposizione precoce a sistemi algoritmici non trasparenti può alterare il processo di formazione della personalità e di autodeterminazione della persona in divenire e quindi anche del futuro cittadino.

L'art. 4 della legge, rubricato "Principi in materia di informazione e di riservatezza dei dati personali", entra nel merito del rapporto tra tecnologie di AI e trattamento dei dati. Il secondo comma stabilisce in modo perentorio che l'utilizzo di sistemi di intelligenza artificiale deve garantire il trattamento lecito, corretto e trasparente dei dati personali, in conformità al diritto dell'Unione europea, aggiungendo che le informazioni e le comunicazioni relative al trattamento devono essere rese con un linguaggio "chiaro e semplice".

Nel caso del genitore che agisce per conto del minore di quattordici anni, l'obbligo di chiarezza diventa cruciale. Se l'informativa è redatta in termini eccessivamente tecnici, ambigui o se occulta la reale finalità del trattamento (ad esempio, l'utilizzo dei dati per l'addestramento di modelli generativi senza specificarlo), il presupposto della "consapevolezza" viene meno⁷⁸.

La legge specifica soglie di età precise che si coordinano con l'art. 8 del GDPR e l'art. 2-*quiquies* del Codice Privacy. L'interazione tra i due commi dell'articolo 4 evidenzia che la validità del consenso è indissolubilmente legata alla qualità dell'informativa. Se l'informativa rivolta al genitore non è chiara, il consenso prestato viola sia l'articolo 4 della legge 132/2025 (per mancata trasparenza specifica sui sistemi IA) sia il GDPR (per mancanza

⁷⁶ Vedi A. ALPINI e S. VILAR GONZALEZ, *La tutela dei minori nell'ambiente digitale: un confronto italo-spagnolo*, in *Le Corti fiorentine*, 1-3, 2025, 3 ss.

⁷⁷ Su questi temi, per tutti, v. O. POLLICINO e P. DUNN, *Intelligenza artificiale e democrazia. Opportunità e rischi di disinformazione e discriminazione*, Milano, 2024; P.F. BRESCIANI e M. PALMIRANI, *AI Act and National Parliaments: How the EU is Regulating Democracy in the Digital Era*, in *Ragion pratica*, 2025, 249 ss.

⁷⁸ Cfr. R. SENIGAGLIA, *Dimensione onlife, famiglia e incapacità dei genitori di assolvere i loro compiti*, in *Dir. succ. fam.*, 2, 2025, 511 ss.



del requisito di “consenso informato”). Ne deriva la nullità del contratto poiché entrambe le fonti pongono l'informazione come elemento costitutivo della validità del consenso, atteso che senza informazione non vi potrebbe essere consapevolezza.

A fronte di un sistema di “capacità funzionali” legate a soglie di età diversificate e soprattutto alle peculiarità dell'ambiente digitale, l'art. 1425 c.c. svolge una funzione di ultima istanza. Se un minore di 14 anni accede ad un sistema di AI mentendo sull'età (*age spoofing*) e conclude un contratto, l'annullamento potrebbe essere il rimedio più adeguato, salvo l'art. 1426 c.c. Al contrario, se il consenso del genitore è inconsapevolmente prestato a causa della mancanza di una informativa chiara sul funzionamento del sistema di AI e tale consenso risulta invalido, non si può escludere la nullità del relativo contratto. Del resto, anche nell'ipotesi di mancanza del consenso del genitore per il figlio minore di 14 anni si possono dare dei casi in cui l'annullamento del contratto non sia il rimedio che meglio tutela l'interesse del minore, considerato che si tratterebbe di salvaguardare i medesimi valori sottesi all'ipotesi in cui il minore ultra quattordicenne presta il consenso inconsapevolmente ex art. 4, l. 132/2025.

L'art. 4, comma 4 stabilisce che il minore (14-18 anni) può prestare il consenso «purché» le informazioni siano chiare e comprensibili. Se la piattaforma viola questo obbligo, il minore non soltanto torna ad essere considerato, per quell'atto specifico, un soggetto legalmente incapace, ma anche inconsapevole e dunque meritevole della protezione più ampia.

Vediamo qualche caso che può verificarsi.

a) Abbonamenti a sistemi di AI generativa con *Dark Patterns*⁷⁹.

Un minore di 15 anni si iscrive a un servizio di creazione di immagini tramite AI. L'interfaccia utilizza tecniche di *overloading* (un eccesso di informazioni tecniche) o *skipping* (percorsi che distolgono l'attenzione dalle clausole sulla *privacy*), portandolo ad accettare un abbonamento che si rinnova automaticamente dopo un periodo di prova gratuito.

b) Servizi di *Chatbot* e “profilazione occulta”⁸⁰.

Il minore interagisce con un assistente virtuale (es. stile Replika) che promette supporto nello studio. L'informativa non chiarisce in modo comprensibile che l'AI analizza i sentimenti e le fragilità del ragazzo per creare un profilo psicometrico vendibile a terzi.

c) Iscrizione ai *Social Media* tramite “base contrattuale”⁸¹.

Alcune piattaforme eludono il limite dei 14 anni sostenendo che il trattamento dei dati sia “necessario all'esecuzione di un contratto”, anziché basato sul consenso. È difficile per un minore cogliere il senso delle condizioni

⁷⁹ B. SIRGIOVANNI, *Il diritto di accesso ai dati e il divieto di dark pattern*, in *Giur. it.*, 2026, 2, 481 ss.; G. VERSACI, *Consenso al trattamento dei dati personali e “dark patterns” tra opzionalità e condizionalità*, in *Nuove leggi civ. comm.*, 2022, 1130 ss.

⁸⁰ Sui problemi connessi alla profilazione, v. A. AMIDEI, *La tutela del consumatore “profilato”: obblighi informativi e asimmetrie negoziali*, in *Giur. it.*, 2025, 461 ss.; C. ALVISI, *Profilazione automatizzata, discriminazione contrattuale e rimedi civilistici*, in *Annali Sisdic*, 2024, 11, 11 ss.

⁸¹ C. PERLINGIERI, *Profili civilistici*, cit., 68; S. THOBANI, *Il consenso al trattamento dei dati come condizione per la fruizione di servizi online*, in C. PERLINGIERI e L. RUGGERI (a cura di), *Internet e diritto civile*, Napoli, 2015, 459 ss.

contrattuali ovvero che sta scambiando i dati personali con l'accesso al servizio.

d) Micro-transazioni e *Gaming Online* (Bait and Switch)⁸².

In molti videogiochi (es. Fortnite), il minore viene condizionato da interfacce studiate per spingerlo a cliccare ripetutamente su pulsanti che portano all'acquisto di "valuta virtuale" o "skin". Se il processo di acquisto nasconde i dettagli economici o utilizza un linguaggio ambiguo per simulare una vincita anziché un acquisto, il minore non può percepire il valore economico dell'operazione.

e) Cessione involontaria del Diritto d'Autore⁸³.

Un minore pubblica contenuti originali (video, testi) su una piattaforma AI che, tra le pieghe di clausole non accessibili, prevede la cessione esclusiva dei diritti di sfruttamento economico dell'opera.

L'art. 1425 c.c. prevede che gli atti compiuti dall'incapace siano annullabili, per lasciare ai genitori la facoltà di decidere se l'atto sia stato comunque utile al minore o se debba essere rimosso.

Quando un contraente (la piattaforma) viola un obbligo di informazione o di trasparenza, sta violando una regola di comportamento (buona fede precontrattuale), con la conseguenza che la violazione di tali obblighi determinerebbe la sua annullabilità per vizio del consenso.

Tuttavia, se la violazione della trasparenza da parte della piattaforma AI è massiva e sistematica (es. uso di *dark patterns*), il giudice, alla luce del DSA e del diritto dei consumi, potrebbe dichiarare la nullità delle singole clausole oscure a vantaggio del minore, mantenendo valido il resto del contratto se favorevole all'utente⁸⁴.

L'art. 4, in linea con l'*AI Act* europeo, non si limita a dettare istruzioni tecniche, ma promuove una visione antropocentrica dell'AI basata sulla tutela della dignità umana e dei diritti fondamentali. Con la conseguenza che se la "trasparenza algoritmica" e la "conoscibilità dei rischi" sono considerate pilastri per il corretto sviluppo della personalità del minore (artt. 2 e 3 Cost.), esse configurano norme imperative di ordine pubblico. Ne deriva che la loro violazione non colpirebbe solo il "comportamento" della piattaforma, ma renderebbe l'intero contratto nullo ex art. 1418, comma 1, c.c., in quanto contrario a un diritto inviolabile ovvero la protezione dell'infanzia (nella rete) e dunque il libero e pieno sviluppo della persona umana⁸⁵.

⁸² A. FACHECHI, "Marketing" aggressivo e microtransazioni "in-game": modelli di tutela, in *Nuovo Dir. Soc.* 2025, pp 198 ss.; M. MAGALDI, "Gaming" tra interessi del mercato e tutela della persona, in *Riv. dir. impr.*, 2024, 3, 617 ss.

⁸³ Cfr. E. ANDREOLA, *Il minore artista nell'era digitale*, in *Famiglia*, 2024, 6, 751 ss.

⁸⁴ G. PERLINGIERI, *L'inesistenza della distinzione tra regole di comportamento e di validità nel diritto italo-europeo*, Napoli, 2013, 51 ss., ma già anche ID., *La convalida delle nullità di protezione e la sanatoria dei negozi giuridici*, Napoli, 2011, 57 ss. Su questa scia: A. ALPINI, *I vizi del consenso fra contratto e trattamento dei dati: la riconoscibilità dell'errore*, in *Pers. merc.*, 2022, 2, 209 ss., spec. 220.

⁸⁵ G. PERLINGIERI, *In tema di ordine pubblico*, in *Rass. dir. civ.*, 2012, 1390. Vedi anche ID., *Regole e comportamenti nella formazione del contratto. Una rilettura dell'art. 1337 codice civile*, Napoli, 2003, 29 ss.

CFR. M. MANTOVANI, *Vizi incompleti del contratto e rimedio risarcitorio*, Torino, 1995 e già: F. BENATTI, *Culpa in contraendo*, 1987, 298; G. VETTORI, *Anomalie e tutele nei con-*

Se la piattaforma non fornisce informazioni chiare, la maggiore età digitale del quattordicenne non si “attiva”. In questa prospettiva, si tratta non solo di una volontà viziata (che porterebbe all’annullabilità), ma della mancanza di capacità speciale in capo al soggetto per quell’atto specifico. Senza capacità e senza una reale rappresentazione dell’oggetto (oscurato da un linguaggio complesso), verrebbe a mancare il fondamento stesso del contratto.

Il genitore non è sempre nelle condizioni materiali di monitorare ogni singola accettazione di “Termini e Condizioni” fatta dal figlio. Di conseguenza, l’annullabilità, essendo prescrivibile e richiedendo un’iniziativa attiva del genitore, rischia di restare una “tigre di carta” contro le *Big Tech*. La nullità, essendo imprescrivibile e rilevabile d’ufficio, è il rimedio che garantisce l’effettività della tutela richiesta dalla legge 132/2025 e dal GDPR. A tale proposito, Federprivacy sostiene già che i contratti che eludono i limiti di età tramite basi contrattuali oscure debbano essere considerati radicalmente nulli⁸⁶.

12. Considerazioni conclusive

L’interferenza di sistemi algoritmici opachi trasforma il processo di negoziazione in un’interazione asimmetrica dove la macchina non è un semplice strumento, ma un agente capace di influenzare i processi cognitivi⁸⁷. L’AI può operare come una *black box*, rendendo impossibile per il contraente umano comprendere i fattori decisivi che hanno condotto a un determinato *output* o proposta contrattuale⁸⁸. In questo scenario, il concetto di “consapevolezza” è non soltanto un mero stato psicologico interno, ma un bene giuridico la protezione del quale è necessaria per garantire la tenuta del sistema sociale e democratico.

Mentre il rimedio dell’annullabilità per proteggere la specifica volontà del singolo contraente interviene *ex post*, l’AI Act adotta un approccio basato sul rischio (*risk-based approach*) che mira a una tutela *ex ante*⁸⁹. Questa divergenza metodologica potrebbe sollevare il dubbio che l’attenzione del

tratti di distribuzione fra imprese. *Diritto dei contratti e regole di concorrenza*, Milano, 1983, 68 ss.

⁸⁶ Vedi <https://www.federprivacy.org/informazione/societa/minori-e-social-network-in-italia-le-contraddizioni-di-un-sistema-di-tutela-mai-applicato-dal-garante-privacy>.

⁸⁷ «In altri termini, vengono intaccati i meccanismi attraverso i quali la volontà si forma nel tempo»: B. PANATTONI, *Condizionamenti e manipolazioni nell’era digitale. Il divieto europeo di pratiche di Intelligenza Artificiale “manipolative”*, in *Dir. pen. proc.*, 2024, 527. V. anche A.C. NAZZARO, *Soggettività dell’avatar tra profilazione e identità personale*, in *Tecn. dir.*, 2024, 1, 135 ss.

⁸⁸ Y. BATHAEE, *The artificial intelligence black box and the failure of intent and causation*, in *Harvard J. L. Techn.*, 2018, 31(2), 936; E. PELLECCIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell’algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civ. comm.*, 2018, 5, 1210 ss.; F. PASQUALE, *The Black Box society. The secret Algorithms that Control Money and Information*, Harvard, 2015, *passim*.

⁸⁹ Nella stessa prospettiva preventiva, L. AULINO, *Consenso al trattamento dei dati e carenza di consapevolezza: il “legal design” come un rimedio “ex ante”*, in *Diritto inf.*, 2020, 2, 303 ss.

legislatore europeo per i “rischi sistemici” finisca per depauperare la tutela della persona fisica, frammentandola in una serie di obblighi di conformità tecnica. Tuttavia, l’analisi delle pratiche vietate suggerisce che il rischio sistemico sia la proiezione macroscopica della lesione individuale: un sistema che manipola la collettività è intrinsecamente un sistema che lede la libertà negoziale di ogni singolo componente di tale collettività.

L’art. 5 dell’*AI Act* vieta espressamente le pratiche di AI che utilizzano tecniche subliminali o manipolative volte a distorcere materialmente il comportamento di una persona. Tali ipotesi sembrano presentare una sovrapposizione concettuale con il dolo (art. 1439 c.c.), inteso come l’insieme di raggi giri volti a indurre una parte in errore per ottenerne il consenso.

Tuttavia, nell’ambito dei sistemi di AI, la manipolazione può avvenire senza che vi sia una specifica intenzione malevola istantanea del *deployer*, essendo spesso il risultato di un’ottimizzazione algoritmica volta alla massimizzazione dell’*engagement* o del profitto⁹⁰.

Il dolo si concentra sull’attività ingannatoria del contraente o del terzo, mentre l’art. 5, lett. a) dell’*AI Act* colpisce la potenzialità distorsiva del mezzo tecnologico in sé, a prescindere dalla prova di un raggiro nel senso classico del termine. La tecnica subliminale agisce sotto la soglia della coscienza, eludendo la possibilità stessa di esercitare la facoltà di discernimento, configurando così una lesione più grave del semplice errore indotto.

Gran parte delle condotte che l’*AI Act* qualifica come manipolative potrebbero essere ricondotte alla nozione di dolo se interpretata in senso evolutivo, poiché la figura del raggiro consente di includervi lo sfruttamento dei *bias* cognitivi operato dagli algoritmi di *neuromarketing*.

L’art. 5, lett. b) vieta lo sfruttamento delle vulnerabilità di persone o gruppi a causa della loro età, disabilità o situazione socio-economica. Nel codice civile, tali situazioni sono protette attraverso l’annullamento per incapacità naturale (art. 428 c.c.) o la disciplina dell’errore sulle qualità personali del contraente, qualora essenziali e riconoscibili (artt. 1428-1429 c.c.).

L’*AI Act* introduce, però, il concetto di “vulnerabilità digitale”, una condizione relazionale che si aggiunge alla vulnerabilità del mondo analogico⁹¹. Si tratta di una “incapacità artificiale” non naturale, ovvero causata dall’uomo se pur applicata attraverso le macchine. Un sistema di AI capace di mappare in tempo reale le debolezze emotive di un utente per proporgli prodotti complessi non solo “induce in errore”, ma soprattutto opera una prevaricazione tecnologica che svuota di significato la volontà negoziale⁹².

Sembra, dunque, che ad essere richiamato all’attenzione sia l’istituto della violenza più che quello del dolo e dell’errore. Il vizio della volontà può

⁹⁰ Sul punto, con particolare riferimento agli acquisti *in game* rientranti tra le pratiche commerciali aggressive, vedi A. GORGONI, *Protezione*, cit., 1169 ss.

⁹¹ Sulla correlazione tra vulnerabilità e dimensione *online*, v. S. TOMMASI, “*Neuromarketing*” *discriminatorio e mercato digitale: il ruolo del “Digital Services Act” e dell’“Artificial Intelligence Act”*, in *Dir. econ.*, 2024, 3, 47 ss.; F. VINCENZI, “*Neuromarketing*” e “*web*”: un connubio legale?, in *Cyberspazio Dir.*, 2017, 3, 615 ss.

⁹² A tal proposito va sottolineato che la distinzione tra tutela della volontà e rischio sistemico appare qui artificiosa: lo sfruttamento sistematico delle vulnerabilità è al contempo un rischio per la stabilità sociale e una lesione immediata dell’autonomia individuale.



assumere nella violenza, sia fisica sia psicologica, un grado tale da annullare del tutto la volontà dell'essere umano⁹³.

La violenza assoluta, intesa come coercizione fisica che esclude totalmente la volontà, provoca la nullità del contratto per mancanza dell'elemento essenziale dell'accordo. Questa sanzione radicale riflette la necessità di disconoscere qualsiasi effetto a un atto che è tale solo nell'apparenza materiale, ma non nell'essenza giuridica. La violenza psicologica o morale, pur agendo sulla psiche del soggetto e non sui suoi muscoli, costituisce la forma più comune di violenza negoziale. Essa provoca l'annullabilità del contratto, consentendo alla vittima di eliminare gli effetti di un accordo estorto con la minaccia di un male ingiusto e notevole. Tuttavia, quando la pressione psichica è tale da annientare la libertà decisionale, essa può essere equiparata alla violenza assoluta, portando alla nullità per mancanza di consenso. Del resto la costrizione è stata interpretata anche come «condizionamento indebito della volontà»⁹⁴. Questa categoria, emersa con forza nel diritto dei consumi e nella disciplina della circonvenzione di incapace, permette di sanzionare condotte che abusano della vulnerabilità altrui o esercitano pressioni sistematiche e aggressive, limitando la capacità di autodeterminazione consapevole. In definitiva, la disciplina dell'invalidità per violenza e condizionamento mira non solo a proteggere il patrimonio del singolo contraente, ma a salvaguardare la dignità della persona e la correttezza del mercato, assicurando che ogni vincolo contrattuale sia il frutto di un atto di libertà e non di un abuso di potere.

Il valore sotteso al rimedio della nullità nelle ipotesi considerate di violenza assoluta è quello di garantire la libertà, l'integrità del processo motivazionale dell'essere umano e dunque la sua libertà di scelta, di espressione e in generale di esplicazione della sua personalità in modo pieno e libero. Un diritto inviolabile della dignità umana che assume un significato ancora più pregnante di fronte ad un sistema algoritmico⁹⁵.

Del resto, la conformità richiesta dall'AI Act non esaurisce le ipotesi da tutelare. Se un fornitore rispetta tutti i requisiti formali ma il sistema, nel caso concreto, manipola comunque l'utente, il solo rispetto dell'AI Act non può escludere l'invalidità del contratto.

In conclusione, l'indagine conferma che la distinzione tra volontà negoziale e rischi sistemici non deve essere letta come una separazione di finalità. Entrambi i sistemi mirano a proteggere la persona umana nella sua capacità di autodeterminarsi in modo consapevole e libero: ciò che viene leso è sempre la consapevolezza dell'individuo.

In questa prospettiva, l'art. 5 dell'AI Act è non una norma aliena al diritto civile, ma ne costituisce l'aggiornamento necessario per far fronte alle

⁹³ Cfr. D. RUSSO, *op. cit.*, 164.

⁹⁴ Vedi L. TAFARO, *Neuroscienze e diritto civile: nuove prospettive*, in *Riv. biodir.*, 2017, 257 ss.; ma già EAD., *Neuromarketing e tutela del consenso*, Napoli, 2018. Vedi altresì E. TUCCARI, *Neuromarketing: un'asistematica disciplina...oltre il consenso?*, in *Pers. merc.*, 2024, 511 e R. MONTINARO, *Riconoscimento delle emozioni e marketing personalizzato*, in *Pers. merc.*, 2024, 847.

⁹⁵ P. PERLINGIERI, *Diritto civile e Intelligenza Artificiale*, cit., 137; S. SIGNORATO, *Il diritto a decisioni penali non basate esclusivamente su trattamenti automatizzati: un nuovo diritto derivante dal rispetto della dignità umana*, in *Riv. dir. proc.*, 2021, 09.

sfide della manipolazione algoritmica, garantendo che il contratto resti un atto di volontà e non una mera risposta a uno stimolo tecnologico preordinato. La persona umana, protetta nella sua dignità, resta il fine ultimo di ogni rimedio, sia esso volto a mitigare un rischio collettivo o a riparare un torto individuale⁹⁶.

Ne deriva che la consapevolezza assurge a principio di ordine pubblico intorno al quale costruire un sistema effettivo di tutela.

Le tecniche algoritmiche che annullano la consapevolezza provocano un vizio della volontà che si traduce in un illecito di ordine pubblico⁹⁷. Se la manipolazione è tale da incidere sulla dignità, il rimedio dell'annullabilità (rimesso alla parte e prescrivibile) si rivela insufficiente; è necessaria la nullità per espungere dal mercato pratiche che minano le basi della convivenza democratica.

Parimenti, la tutela dei minori non può essere affidata solo all'azione di annullamento per incapacità. La legge italiana, integrando i requisiti di trasparenza del GDPR e dell'*AI Act*, sposta il baricentro verso la nullità del consenso e del contratto quando l'informativa al genitore o al minore non mette nelle condizioni di poter agire consapevolmente. Sì che la capacità digitale dipende dalla verifica non soltanto della soglia anagrafica prevista ma anche della comprensibilità per i minori dei rischi conseguenti all'uso dei sistemi digitali. La mancanza di una informazione chiara e comprensibile ai minori espone inconsapevolmente i destinatari più vulnerabili a tecniche di condizionamento della volontà.

La sfida futura risiederà nella capacità degli interpreti e in particolare dei giudici di decodificare il funzionamento dei sistemi per distinguere, nel caso concreto, tra un semplice inganno (annullabile) e una manipolazione lesiva della dignità (nulla), considerando che nell'ambiente digitale la linea di confine è tracciata dalla trasparenza e dalla reale possibilità per l'umano di esercitare una supervisione significativa. La legge italiana, affermando la "riserva di umanità", pone l'Italia all'avanguardia in questo processo di "civilizzazione del digitale".

⁹⁶ Sul valore centrale della dignità umana, v. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, II, *Fonti e interpretazione*, 4^a ed., Napoli, 2020, p. 20 ss.; ID., *La personalità umana*, cit., p. 12 ss.; ID., *Principio personalista, dignità umana e rapporti civili*, in *Ann. Sisdic*, 2020, p. 1 ss., ora anche in ID., *Lezioni* (1969-2019), III, Napoli, 2020, 411 ss. In argomento, v. anche S. COTTA, *Soggetto di diritto*, in *Enc. dir.*, XLII, Milano, 1990, 1220; L. LONARDO, *Il valore della dignità della persona nell'ordinamento italiano*, in *Rass. dir. civ.*, 2011, 773 ss.

⁹⁷ G. PERLINGIERI, *Negozi illeciti e negozi illegali. Una incerta distinzione sul piano degli effetti*, Napoli, 2003, 21, ss.; ID., *L'inesistenza della distinzione tra regole di comportamento e di validità nel diritto italo-europeo*, Napoli, 2013, 31 ss. e spec. 84 ove si invita l'interprete a valutare sempre l'incidenza del singolo vizio nell'area del valore e a porre attenzione al "giusto rimedio". Cfr. G. VETTORI, *Efficacia e opponibilità del patto di preferenza*, Roma, 1988, 144; ID., *Diritto privato e ordinamento comunitario*, Milano, 2009, 252 ss. e 271 ss. secondo il quale: «la disciplina dell'atto e dei congegni è diversa, come autonome e cumulabili sono le due valutazioni di validità e di responsabilità».



