



I A I C



DGBIC



CREDA

DIRITTO MERCATO TECNOLOGIA

FONDATA E DIRETTA DA

Alberto M. Gambino

COMITATO DI DIREZIONE

Valeria Falce, Giusella Finocchiaro, Oreste Pollicino,
Giorgio Resta, Salvatore Sica

2 settembre 2026

Persona, dato, mercato. La protezione dei dati personali alla prova
dell'intelligenza artificiale tra modello europeo e modello statunitense

Riccardo Jovine

COMITATO SCIENTIFICO

Guido Alpa †, Fernando Bocchini, Giovanni Comandè, Gianluca Contaldi,
Vincenzo Di Cataldo, Giorgio Floridia, Gianpiero Gamaleri, Gustavo Ghidini,
Andrea Guaccero, Mario Libertini, Francesco Macario, Roberto Mastroianni,
Giorgio Meo, Cesare Mirabelli, Enrico Moscati, Alberto Musso, Luca Nivarra,
Gustavo Olivieri, Cristoforo Osti, Roberto Pardolesi, Giuliana Scognamiglio,
Giuseppe Sena, Vincenzo Zeno-Zencovich, Andrea Zoppini

E

Margarita Castilla Barea, Cristophe Geiger, Reto Hilty, Ian Kerr, Jay P. Kesan,
David Lametti, Fiona MacMillan, Maximiliano Marzetti, Ana Ramalho,
Maria Pàz Garcia Rubio, Patrick Van Eecke, Hong Xue



Nuova
Editrice
Universitaria

La rivista è stata fondata nel 2009 da Alberto M. Gambino ed è oggi pubblicata dall'Accademia Italiana del Codice di Internet (IAIC) sotto gli auspici del Ministero dei beni e delle attività culturali e del turismo - Direzione generale biblioteche e istituti culturali (DGBIC) e dell'Università Europea di Roma con il Centro di Ricerca di Eccellenza del Diritto d'Autore (CREDA). Tutti i diritti sono dell'IAIC.

Comitato dei Valutazione Scientifica

EMANUELA AREZZO (Un. Teramo), EMANUELE BILOTTI (Un. Europea di Roma), FERNANDO BOCCHINI (Un. Federico II), ROBERTO BOCCHINI (Un. Parthenope), ORESTE CALLIANO (Un. Torino), LOREDANA CARPENTIERI (Un. Parthenope), LUCIANA D'ACUNTO (Un. Federico II), VIRGILIO D'ANTONIO (Un. Salerno), FRANCESCO DI CIOMMO (Luiss), MARILENA FILIPPELLI (Un. Tuscia), CESARE GALLI (Un. Parma), MARCO MAUGERI (Un. Europea di Roma), ENRICO MINERVINI (Seconda Un.), GILBERTO NAVA (Un. Europea di Roma), MARIA CECILIA PAGLIETTI (Un. Roma Tre), ANNA PAPA (Un. Parthenope), ANDREA RENDA (Un. Cattolica), ANNARITA RICCI (Un. Chieti), FRANCESCO RICCI (Un. LUM), GIOVANNI MARIA RICCIO (Un. Salerno), CRISTINA SCHEPISI (Un. Parthenope), BENEDETTA SIRGIOVANNI (Un. Tor Vergata), GIORGIO SPEDICATO (Un. Bologna), ANTONELLA TARTAGLIA POLCINI (Un. Sannio), RAFFAELE TREQUATTRINI (Un. Cassino), DANIELA VALENTINO (Un. Salerno), FILIPPO VARI (Un. Europea di Roma), ALESSIO ZACCARIA (Un. Verona).

Norme di autodisciplina

1. La pubblicazione dei contributi sulla rivista "Diritto Mercato Tecnologia" è subordinata alla presentazione da parte di almeno un membro del Comitato di Direzione o del Comitato Scientifico e al giudizio positivo di almeno un membro del Comitato per la Valutazione Scientifica, scelto per rotazione all'interno del medesimo, tenuto conto dell'area tematica del contributo. I contributi in lingua diversa dall'italiano potranno essere affidati per il referaggio ai componenti del Comitato Scientifico Internazionale. In caso di pareri contrastanti il Comitato di Direzione assume la responsabilità circa la pubblicazione.

2. Il singolo contributo è inviato al valutatore senza notizia dell'identità dell'autore.

3. L'identità del valutatore è coperta da anonimato.

4. Nel caso che il valutatore esprima un giudizio positivo condizionato a revisione o modifica del contributo, il Comitato di Direzione autorizza la pubblicazione solo a seguito dell'adeguamento del saggio.

La Rivista adotta un Codice etico e di buone prassi della pubblicazione scientifica conforme agli standard elaborati dal Committee on Publication Ethics (COPE): Best Practice Guidelines for Journal Editors.

Comitato di Redazione — www.dimt.it — dimt@unier.it

ANTONINA ASTONE, MARCO BASSINI, CHANTAL BOMPRESZI, VALENTINA DI GREGORIO, GIORGIO GIANNONE CODIGLIONE, FERNANDA FAINI, MASSIMO FARINA, ILARIA GARACI, SILVIA MARTINELLI, DAVIDE MULA (Coordiatore), ALESSIO PERSIANI, MARTINA PROVENZANO (Vice-Coodiatore), MARIA PIA PIGNALOSA, MATILDE RATTI, ANDREA STAZI (Coordiatore)

Sede della Redazione

Accademia Italiana del Codice di Internet, Via dei Tre Orologi 14/a, 00197 Roma, tel. 06.8088355, fax 06.8070483, www.iaic.it, info@iaic.it

PERSONA, DATO, MERCATO. LA PROTEZIONE DEI DATI PERSONALI ALLA PROVA DELL'INTELLIGENZA ARTIFICIALE TRA MODELLO EUROPEO E MODELLO STATUNITENSE

Riccardo Jovine*

SOMMARIO: 1. Introduzione. L'intelligenza artificiale e il diritto privato dei dati – 2. Due tradizioni a confronto: il dato come diritto della personalità nel modello europeo e come *commodity* nel modello statunitense – 3. La dimensione collettiva della privacy nell'era dei *Big Data*: profilazione, *group privacy* e i limiti della tutela individuale – 4. La convergenza con il diritto dei consumatori: azioni di classe, trapianti giuridici e l'esperienza italiana (dal caso *Facebook–AGCM a Meta c. Bundeskartellamt*) – 5. Dal rimedio alla prevenzione: l'approccio proattivo europeo, l'AI Act e il Digital Omnibus. Considerazioni conclusive

ABSTRACT: Il presente contributo analizza, con modalità comparatistica, l'impatto dell'intelligenza artificiale sul diritto privato dei dati personali, a partire dalla divergenza strutturale fra il modello europeo, che considera la protezione del dato come un diritto della personalità garantito da una regolazione generale e preventiva, e il modello statunitense, che tratta il dato come *commodity* affidata all'autonomia contrattuale e a tutele settoriali di matrice rimediabile. L'analisi svolta giunge a sostenere che le sfide poste dall'IA, e in particolare la dimensione collettiva del pregiudizio algoritmico prodotta dalla profilazione a livello di gruppo eludendo le tutele individuali, mettano in moto un processo di convergenza tra i due sistemi, secondo dinamiche di trapianto e ricezione di cui l'esperienza italiana costituisce un laboratorio di riferimento: dalla riuscita ricezione della disciplina europea dei dati alla vicenda Facebook–AGCM, che ha anticipato la complementarità tra protezio-

* Professore a contratto di Diritto Comparato delle Biotecnologie presso l'Università San Raffaele Roma. Conosciuto anche come: Riccardo Jovine. ORCID iD: 0009-0009-1302-4873. Email: riccardo.jovine@uniroma5.it

ne dei dati, diritto dei consumatori e diritto della concorrenza, successivamente consacrata dal legislatore e dalla Corte di giustizia nella controversia *Meta c. Bundeskartellamt*. L'analisi si conclude interrogando la tenuta dell'approccio proattivo europeo alla luce dell'AI Act, del Regolamento (UE) 2026/1744 e della legge 132/2025: la scommessa di governare il rischio tecnologico in anticipo sul danno è ormai entrata nella fase di prova, ma la persona, non il mercato né la macchina, rimane l'ineludibile punto di riferimento di ogni regola.

1. Introduzione. L'intelligenza artificiale e il diritto privato dei dati

Per valutare l'impatto dell'intelligenza artificiale nella sfera del diritto privato non serve alcun esercizio di fantascientifica immaginazione. Non occorrono scenari di macchine dotate di coscienza o di capacità sovrumane, ma basta osservare ciò che già oggi sta accadendo nella quotidianità delle relazioni giuridiche. Assistenti vocali che raccolgono dati all'interno delle abitazioni, processi di profilazione che selezionano i destinatari di messaggi pubblicitari e di offerte commerciali, algoritmi di *scoring* che condizionano l'accesso al credito, modelli generativi addestrati su immense quantità di dati personali: in ognuna di tali fattispecie l'intelligenza artificiale incide su categorie fondamentali del diritto privato, il consenso, il contratto, la responsabilità, i diritti della personalità, e lo fa anzitutto attraverso il trattamento dei dati personali¹. Il diritto privato dei dati costituisce dunque il terreno di elezione per verificare la tenuta delle tradizionali categorie del diritto di fronte al veloce cambiamento tecnologico in atto².

¹ U. PAGALLO, *Data Protection in EU and US Laws and AI: What Legal Changes We Should Expect in the Foreseeable Future?*, in E. Lim, P. Morgan (eds.), *The Cambridge Handbook of Private Law and Artificial Intelligence*, Cambridge University Press, Cambridge, 2024, pp. 599 ss., dove si mette in evidenza che una stessa tecnologia pone problematiche giuridiche diverse in relazione all'ordinamento considerato, e si individua nel dinamismo della ricezione e dei trapianti la chiave di lettura per valutare le convergenze in atto tra il diritto europeo e il diritto statunitense.

² G. ALPA, *L'intelligenza artificiale. Il contesto giuridico*, Mucchi, Modena, 2021, il quale rileva che l'applicazione dell'intelligenza artificiale agli scambi commerciali, alla raccolta e

Lo scenario è ormai noto. Le società contemporanee non si limitano ad utilizzare le tecnologie dell'informazione, ma dipendono da esse al punto tale che l'utilizzo dei dati è diventato una risorsa essenziale del sistema socio-economico, in base a un'evoluzione che la dottrina ha descritto a partire dagli anni Novanta del secolo scorso, quando l'attenzione degli studiosi iniziò a concentrarsi sulle regole di accesso, controllo e protezione dell'informazione nel contesto digitale³. Fu in quella stagione che iniziò a maturare, anche nella riflessione nordamericana, la consapevolezza che la struttura tecnologica è essa stessa una forma di regolazione, il *code is law* di Lawrence Lessig e la *lex informatica* di Joel Reidenberg⁴, e che il passaggio dal diritto alla riservatezza al diritto alla tutela dei dati personali rappresenta una delle più radicali trasformazioni del diritto privato contemporaneo⁵.

al trattamento dei dati personali e all'utilizzo di robot pone il giurista di fronte alla necessità di individuare dei modelli giuridici capaci di qualificarne gli effetti e di trovare dei rimedi per compensarne i danni, in un contesto nel quale l'Unione europea ha puntato a coniugare il sostegno allo sviluppo tecnologico e la tutela dei diritti della persona.

³ S. RODOTÀ, *Tecnologie e diritti*, il Mulino, Bologna, 1995, dove si teorizza la transizione dalla riservatezza come fattore di segretezza alla privacy come diritto di controllo dell'interessato sulla diffusione delle informazioni che lo riguardano, precorrendo la definizione della tutela dei dati come diritto fondamentale autonomo; prospettiva successivamente sviluppata in ID., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, dove la protezione della persona nel contesto elettronico è ricondotta al nucleo del costituzionalismo contemporaneo, per contrastare il rischio che l'individuo venga ridotto ad una sorta di "uomo di vetro" trasparente ai poteri pubblici e privati.

⁴ J. L. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, 76, 1998, pp. 553 ss., che è stato il primo a porre in evidenza come le architetture tecnologiche delle reti incorporino delle vere e proprie regole di condotta, in qualche misura analoghe alle norme giuridiche e concorrenti con esse; nella stessa direzione L. LESSIG, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999, con la celebre tesi secondo la quale "il codice è legge": il software condiziona ed orienta i comportamenti al pari, e talora più efficacemente, del diritto, dei mercati e delle regole sociali.

⁵ Per una visione d'insieme di come le tecnologie digitali possano trasformare le regole giuridiche, e in particolare il percorso che conduce dal diritto alla riservatezza al diritto alla tutela dei dati personali fino alla strategia europea sui dati, si veda: G. PASCUZZI, *Il diritto dell'era digitale*, 5ª ed., il Mulino, Bologna, 2020, spec. Parte II, dove si evidenzia come la vicenda dei dati personali rappresenti il paradigma dei radicali mutamenti indotti dalla rivoluzione tecnologica digitale sulle categorie del diritto privato. Si veda anche a tale proposito: A. M. GAMBINO, A. STAZI, D. MULA, *Diritto dell'informatica e della comunicazione*, 3ª ed., Giappichelli, Torino, 2019, pp. 61 ss.

Rispetto a tale scenario ormai consolidato, l'intelligenza artificiale presenta tuttavia un fattore di discontinuità. I sistemi di intelligenza artificiale non sono strumenti che escono dalla fabbrica “chiavi in mano”, identici a sé stessi per l'intera durata del ciclo vitale: sono strumenti che si evolvono attraverso l'interazione con l'ambiente e con le persone, che si alimentano di dati in modo continuo e che, a causa di ciò, sviluppano capacità non del tutto prevedibili nemmeno dai loro sviluppatori. Complessità, opacità, autonomia, apertura, dipendenza dai dati e vulnerabilità sono i fattori che, secondo il parere del gruppo di esperti istituito dalla Commissione europea in materia di responsabilità e nuove tecnologie, provocano un effetto complessivamente dirompente sugli attuali istituti giuridici, nonostante ogni cambiamento, ove isolatamente considerato, possa apparire graduale⁶. Ne risultano investite le nozioni di base della disciplina dei dati. Chi è il “titolare del trattamento” quando l'utilizzatore finale addestra, con il proprio uso, il sistema che lo osserva? Quale “ragionevole aspettativa di riservatezza” può definirsi tale, quando la tecnologia ha la capacità di riplasmare continuamente le aspettative sociali?⁷

A tali domande gli ordinamenti giuridici rispondono in modo diverso. Ed è proprio a questo punto che la prospettiva comparatistica manifesta la propria utilità: una medesima tecnologia, un modello generativo, un assistente personale intelligente, un sistema di raccomandazione, solleva questioni giuridiche diverse, e in qualche caso addirittura opposte, a seconda dell'ordinamento considerato. Nel modello europeo, la tutela dei dati perso-

⁶ EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies*, European Commission, 2019, pp. 11-62, dove sono elencati gli aspetti caratterizzanti delle tecnologie emergenti: complessità, apertura, opacità, autonomia, limitata prevedibilità, dipendenza dai dati e vulnerabilità; con l'avvertenza che, nonostante ogni cambiamento possa sembrare graduale, la sommatoria di ampiezza, frequenza ed effetto congiunto di queste trasformazioni determina un esito dirompente per i regimi di responsabilità esistenti.

⁷ Su tali tematiche, si veda: W. BARFIELD, U. PAGALLO, *Advanced Introduction to Law and Artificial Intelligence*, Edward Elgar, Cheltenham, 2020, i quali elencano le sfide che l'intelligenza artificiale presenta ai diversi ambiti dell'ordinamento giuridico e sottolineano che il carattere adattivo dei sistemi di apprendimento automatico introduce un fattore di instabilità sia nella ripartizione dei ruoli tra l'utilizzatore e il titolare del trattamento, sia nel criterio di ragionevole aspettativa di riservatezza sviluppato dalla giurisprudenza statunitense.

nali viene ritenuta un diritto fondamentale della persona, un'espressione dei diritti della personalità garantita da una regolazione generale e tendenzialmente onnicomprensiva; invece nel modello statunitense prevale una concezione del dato come *commodity*, vale a dire un bene negoziabile che può essere oggetto di autonomia contrattuale e rimesso a tutele di matrice rimediale, settoriali e reattive⁸. L'antitesi tra persona e mercato, tra il dato come espressione della personalità e il dato come *asset* meramente economico, attraversa l'intera materia, ma non la esaurisce: come si vedrà più avanti, le sfide poste dall'intelligenza artificiale, e in particolare la dimensione collettiva assunta dalla tutela nell'era dei *Big Data*, stanno favorendo significative convergenze fra i due modelli, secondo dinamiche di circolazione, trapianto e ricezione di cui il diritto comparato è consapevole da tempo e che l'esperienza italiana conferma in modo esemplare⁹.

Il momento, del resto, si rivela particolarmente propizio per un bilancio. Il quadro normativo europeo è in piena fase di sviluppo: il Regolamento

⁸ La divergenza tra i due modelli è la tematica sviluppata da U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Giuffrè, Milano, 2008, pp. 61 ss., il quale ricostruisce le origini storiche e concettuali di tale divergenza: da un lato la tradizione statunitense della *tort law* e del Quarto Emendamento, caratterizzata da una visione proprietaria e rimediale; dall'altro lato la concezione europea, che considera la tutela dei dati come un diritto della personalità garantito da una disciplina generale del ciclo vitale dell'informazione. Nella letteratura statunitense, si veda: J. Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in *The Yale Law Journal*, 2004, pp. 1153 ss.; e P. M. SCHWARTZ, K. N. PEIFER, *Transatlantic Data Privacy Law*, in *The Georgetown Law Journal*, pp. 121 ss.

⁹ In merito alla tensione tra persona e mercato nella veicolazione degli attributi della personalità, si veda: G. RESTA, *Dignità, persone, mercati*, Giappichelli, Torino, 2014, il quale spiega che la commercializzazione degli attributi immateriali della persona non può essere interpretata soltanto alla luce delle categorie proprietarie, ma richiede un costante bilanciamento tra la logica dignitaria e la logica di mercato: la stessa polarità che attraversa lo statuto giuridico del dato personale; e G. RESTA, *The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives*, in *Tulane European and Civil Law Forum*, 2011, Vol. 26, pp. 33 ss. Per un confronto tra i due modelli nella dimensione transnazionale, si veda: G. RESTA, V. ZENOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTre-Press, Roma, 2016, dove, a partire dalla sentenza Schrems, vengono poste in evidenza l'affermazione di un modello europeo alternativo a quello statunitense e la prevalenza del controllo giurisdizionale sulle intese tra le due sponde dell'Atlantico.

(UE) 2024/1689 sull'intelligenza artificiale (AI Act)¹⁰ è in fase di applicazione graduale, i divieti delle pratiche a rischio inaccettabile sono attivi dal febbraio 2025, le regole sui modelli di intelligenza artificiale per finalità generali dall'agosto 2025, mentre il Regolamento (UE) 2026/1744, adottato nel luglio del 2026, ha differito al mese di dicembre 2027 e al mese di agosto 2028 l'applicazione degli obblighi per i sistemi ad alto rischio, introducendo al tempo stesso nuovi divieti per i sistemi di intelligenza artificiale destinati a generare immagini non consensuali¹¹. Sul versante interno, la legge 23 settembre 2025 n. 132 ha dotato l'Italia di una cornice organica in materia di intelligenza artificiale, tra i primi Stati membri¹². Le considerazioni che seguono muovono da tale scenario: evidenziando in primo luogo le differenze strutturali tra il modello europeo e il modello statunitense, per poi analizzare la dimensione collettiva della tutela, messa in crisi dalla profilazione algoritmica, e la convergenza tra la protezione dei dati e il diritto dei consumatori, con particolare riguardo all'esperienza italiana dei trapianti giuridici. E infine per interrogarsi sulla capacità dell'approccio proattivo europeo di governare la transizione attualmente in atto.

¹⁰ Cfr. Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che fissa regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828. Tale regolamento rappresenta il primo quadro normativo orizzontale al mondo in materia di intelligenza artificiale, basato su un approccio relativo al rischio che stabilisce una gradualità di obblighi in relazione alla pericolosità dei sistemi. Il calendario applicativo è suddiviso ai sensi dell'articolo 113 del Regolamento.

¹¹ Cfr. il Regolamento (UE) 2026/1744 che modifica i Regolamenti (UE) 2024/1689 e (UE) 2018/1139 per quanto concerne la semplificazione attuativa delle regole armonizzate sull'intelligenza artificiale (Omnibus digitale sull'IA) – COM/2025/836 final, finalizzata a ridurre gli oneri di conformità rispetto al ritardo degli standard armonizzati e alla mancata designazione di numerose autorità nazionali.

¹² L. 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale, che definisce la cornice nazionale di *governance* del settore, con l'attribuzione delle funzioni di vigilanza del mercato all'Agenzia per la cybersicurezza nazionale, e interviene, tra l'altro, sulla tutela penale della persona rispetto ai contenuti generati artificialmente.

2. Due tradizioni a confronto: il dato come diritto della personalità nel modello europeo e come *commodity* nel modello statunitense

Privacy e protezione dei dati personali sono due nozioni contigue, ma non coincidenti. Il diritto alla privacy, nella sua tradizionale accezione, tutela il corpo, gli spazi, le comunicazioni e le scelte di autodeterminazione della persona; mentre la protezione dei dati personali tutela le informazioni che la riguardano, in qualsiasi modo esse siano trattate. L'ordinamento giuridico europeo ha sancito la distinzione a livello di diritto primario, dedicando ai suddetti diritti disposizioni separate, gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, e la differenza non è soltanto sistemica: vi sono pregiudizi alla vita privata che non comportano alcun trattamento di dati, come l'attribuzione di una notorietà non voluta o la rappresentazione sotto "falsa luce" della persona, ed esistono all'inverso tutele che prescindono da ogni pregiudizio concreto, come il diritto di ottenere la deindicizzazione di informazioni lecitamente pubblicate¹³. Se la privacy preserva, per riprendere una suggestione "arendtiana", l'opacità della persona e il suo diritto di celarsi allo sguardo altrui, la protezione dei dati personali ruota attorno alla trasparenza del trattamento: chi li raccoglie, per quali finalità e con quali strumenti¹⁴. Da tale trasparenza dipende l'insieme dei diritti che compone lo statuto europeo dell'interessato: accesso, rettifica, cancellazione e opposizione; diritti che il Tribunale federale tedesco ha ricondotto, fin dalla storica

¹³ La distinzione è stabilita dagli articoli 7 (rispetto della vita privata) e 8 (protezione dei dati personali) della Carta dei diritti fondamentali dell'Unione europea. Cfr. CGUE, Grande Sezione, 13 maggio 2014, C-131/12, Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, spec. punti 96 e 99, dove si rileva che il diritto dell'interessato alla deindicizzazione non implica che l'inclusione dell'informazione nei risultati della ricerca generi un danno: la Corte stabilisce una forma di protezione che opera sul piano del controllo dell'informazione, a prescindere da un'eventuale lesione.

¹⁴ In riferimento alla riflessione di Hannah Arendt sulla condizione umana, come strumento per distinguere la tutela dell'opacità della persona (privacy) dalla trasparenza del trattamento (*data protection*), si veda: U. PAGALLO, *On the Principle of Privacy by Design and Its Limits: Technology, Ethics and the Rule of Law*, in S. GUTWIRTH ET AL. (eds.), *European Data Protection: In Good Health?*, Springer, Dordrecht, 2012, il quale osserva che i due paradigmi riflettono logiche speculari: l'una che si riferisce alla sottrazione allo sguardo altrui, l'altra che disciplina la visibilità.

sentenza sul censimento del 1983, al principio di autodeterminazione informativa¹⁵.

Le due forme di tutela, seppure distinte in astratto, convergono continuamente nella prassi. La giurisprudenza della Corte europea dei diritti dell'uomo riconduce entrambe all'articolo 8 CEDU, e non è un caso che, sia nel linguaggio corrente che nel linguaggio legislativo, i due termini vengano utilizzati in modo sostanzialmente intercambiabile. L'esperienza italiana assume un aspetto emblematico: il diritto alla riservatezza, nato come creazione giurisprudenziale in assenza di una previsione codicistica espressa, ha trovato una decisiva consacrazione nella nota pronuncia della Cassazione in merito al caso della principessa Soraya; la disciplina europea è stata successivamente recepita in Italia con la legge 31 dicembre 1996 n. 675 e trasfusa nel d.lgs. 30 giugno 2003 n. 196, universalmente definito "Codice della privacy", nonostante si riferisca alla protezione dei dati personali¹⁶.

Assai diversa è la traiettoria statunitense. La privacy nordamericana nasce infatti come *right to be let alone* nel celebre contributo di Warren e Brandeis¹⁷, ma si sviluppa lungo due direttrici che ne definiscono il carattere: sul piano costituzionale, la tutela contro le "perquisizioni e i sequestri irragionevoli" prevista dal Quarto Emendamento, ancorata dal caso Katz al criterio

¹⁵ Cfr. BVerfG, 15 dicembre 1983 (Volkszählungsurteil): il Tribunale costituzionale federale tedesco, nel dichiarare parzialmente incostituzionali alcune norme della legge federale sul censimento, riconduce agli articoli 1 e 2 della Legge fondamentale tedesca (Grundgesetz) il diritto all'autodeterminazione informativa (*informationelle Selbstbestimmung*): autodeterminazione che viene intesa come diritto del singolo a decidere, in linea di principio, in merito alla comunicazione e alla utilizzazione dei dati che lo riguardano; un principio che eserciterà una marcata influenza sul successivo sviluppo della protezione dei dati personali nel modello europeo.

¹⁶ Cfr. Cass., 27 maggio 1975, n. 2129 e l. 31 dicembre 1996, n. 675 poi riordinata nel d.lgs. 30 giugno 2003, n. 196. Sull'evoluzione della materia e sull'uso ormai consolidato del termine "privacy" per significare la protezione dei dati, si veda: S. SICA, V. ZENOVICH (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, VII ed., Wolters Kluwer-Cedam, Milano, 2026, pp. 297 ss.

¹⁷ S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, Vol. 4, No. 5, pp. 193 ss., dove gli autori teorizzano, come reazione all'invasione della fotografia istantanea e dei media scandalistici, il diritto "ad essere lasciati soli" radicato nella *inviolate personality*: una dimostrazione che anche la tradizione americana ha origine da una matrice personalistica, poi gradualmente reinterpretata in chiave proprietaria e rimediabile.

della ragionevole aspettativa di riservatezza; sul piano privatistico, una tradizione di *tort law* che protegge la persona attraverso formule risarcitorie tipizzate. Su tale impianto si innesta la *third-party doctrine*: chi comunica volontariamente informazioni a terzi, come ad esempio la banca o la compagnia telefonica, rinuncia automaticamente alla protezione costituzionale, in quanto la segretezza costituisce il fondamento della tutela¹⁸. Ne deriva una concezione del dato come bene disponibile, oggetto di scambio e di condizioni contrattuali, più che come espressione della personalità: una *commodity* la cui circolazione è rimessa all'autonomia privata e, ove occorra, è governata da interventi legislativi settoriali e reattivi, dal Privacy Act del 1974 al Video Voyeurism Prevention Act del 2004; interventi, questi ultimi, che costituiscono quasi sempre risposte a scandali, mentre la revisione della dottrina del terzo, avviata dalla Corte Suprema in *Carpenter v. United States* per i dati di localizzazione cellulare, rimane parziale e non ne altera il presupposto di fondo¹⁹.

Il metodo comparativo permette allora di individuare due differenze strutturali. La prima differenza riguarda lo statuto giuridico del dato: un approccio che risulta tendenzialmente proprietario negli Stati Uniti, dove non manca chi teorizza esplicitamente la privacy come *property*²⁰; mentre costituisce

¹⁸ Il criterio della ragionevole aspettativa di riservatezza è stato elaborato da *Katz v. United States*, 389 U.S. 347 (1967), spec. nella *concurring opinion* del giudice Harlan; la *third-party doctrine* è stata sancita da *United States v. Miller*, 425 U.S. 435 (1976) per i documenti bancari, e da *Smith v. Maryland*, 442 U.S. 735 (1979) per i tabulati telefonici: in entrambi i casi la Corte Suprema ha affermato che le informazioni comunicate volontariamente a terzi non sono tutelate dal Quarto Emendamento, saldando la protezione della privacy al requisito della segretezza.

¹⁹ La graduale erosione di tale impianto di fronte allo sviluppo delle tecnologie digitali è attestata da *Kyllo v. United States*, 533 U.S. 27 (2001) sull'utilizzo di termocamere; da *United States v. Jones*, 565 U.S. 400 (2012) sulla localizzazione GPS, dove la *concurring opinion* della giudice Sotomayor mette in discussione la perdurante idoneità della *third-party doctrine* nel contesto digitale, in cui le persone diffondono una rilevante quantità di informazioni su sé stesse a terzi nel corso delle attività quotidiane; e, infine, da *Carpenter v. United States*, 585 U.S. 296 (2018), che limita l'applicazione della *third-party doctrine* ai dati storici di localizzazione cellulare, senza però superarne il principio generale.

²⁰ Si veda: L. LESSIG, *Privacy as Property*, in *Social Research*, 2002, Vol. 69, pp. 247-269, il quale suggerisce di creare un diritto di proprietà individuale sui dati personali al fine di fortificarne il potere negoziale: un parere rappresentativo di un contesto culturale

un diritto della personalità nell'Unione europea, dove la protezione è indisponibile nel suo fondamento e accompagna il dato lungo tutto il suo ciclo vitale. La seconda differenza riguarda la finalità della regolazione: il legislatore europeo, dalla direttiva 95/46/CE al GDPR, ha puntato a disciplinare, in via generale e tecnologicamente neutra, ogni trattamento di dati personali, mitigando il comando verticale attraverso il principio di *accountability* che responsabilizza il titolare con una logica di co-regolazione²¹; il legislatore federale statunitense è intervenuto invece per emergenze e per settori, conferendo ampi spazi all'autoregolamentazione contrattuale e alla gestione dei singoli Stati²². La dottrina italiana ha individuato in modo preciso la posta in gioco: la "rivoluzione dei *Big Data*" mette in tensione le tradizionali categorie civilistiche proprio perché il dato è, al tempo stesso, un attributo della persona e un bene economico, per cui nessuno dei due paradigmi, quello dignitario e quello mercantile, riesce, da solo, a darne conto²³.

L'intelligenza artificiale amplifica le fragilità di entrambi i modelli. Nel modello europeo, i principi di limitazione della finalità e di minimizzazione dei dati confliggono con sistemi tecnologici che apprendono da enormi quantità di informazioni per finalità non del tutto predeterminabili. Un esempio è l'assistente domestico intelligente: il titolare gode di ampi margini

dove la protezione della privacy viene perseguita attraverso gli strumenti del mercato, anziché porre dei limiti al mercato stesso.

²¹ Sul principio di *accountability* di cui all'art. 5, par. 2, GDPR come modello di co-regolazione che tempera l'impianto verticale del sistema europeo, si veda: U. PAGALLO, P. CASANOVAS, R. MADELIN, *The Middle-Out Approach: Assessing Models of Legal Governance in Data Protection, Artificial Intelligence, and the Web of Data*, in *The Theory and Practice of Legislation*, 2019, Vol. 7, p. 1 ss., che indicano una terza via tra autoregolamentazione e regolazione *top-down*.

²² Cfr. Privacy Act (1974), Cable Communications Policy Act (1984), Electronic Communications Privacy Act (1986), HIPAA (1996), Identity Theft and Assumption Deterrence Act (1998), CAN-SPAM Act (2003), Video Voyeurism Prevention Act (2004), HI-TECH Act (2009): leggi di settore, che sono state perlopiù emanate in conseguenza di scandali, e che confermano la qualità frammentaria e rimediabile dell'intervento federale.

²³ V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten Legal Perspectives on the "Big Data Revolution"*, in *Concorrenza e mercato*, 2016, Vol. 23, pp. 29 ss., i quali illustrano l'incidenza dei *Big Data* sulle primarie categorie del diritto privato, dalla titolarità dei dati alla responsabilità, dal consenso alla concorrenza, ponendo in evidenza la tensione crescente fra la qualificazione dei dati personali come diritti della personalità e il loro aumentato valore economico nell'ambito dei mercati digitali.

nello stabilire le finalità; la capacità di riconoscimento vocale consente di raccogliere una quantità ininterrotta di dati, e la stessa distinzione fra titolare del trattamento e utilizzatore finale si fa incerta. Questo è ciò che avviene quando è l'utente ad addestrare, attraverso l'uso, il sistema che lo osserva²⁴. Che il modello europeo punti ad applicare le proprie categorie all'intelligenza artificiale generativa è confermato, da un lato, dal modo in cui il Comitato europeo per la protezione dei dati ha affrontato la tematica dell'anonimato dei modelli e della base giuridica del loro addestramento²⁵; dall'altro, dalla sanzione italiana inflitta ad OpenAI: il Garante ha infatti sanzionato, in fase istruttoria, il fornitore generativo a larga diffusione della società statunitense. Il provvedimento è stato poi annullato in sede giurisdizionale, ma ciò è avvenuto per motivi relativi alla divisione di competenze fra autorità nazionali nel meccanismo dello sportello unico; a conferma, ancora una volta, che la partita si gioca all'interno delle categorie ordinarie del GDPR²⁶. Nel modello statunitense, è la *third-party doctrine* a rivelarsi inuti-

²⁴ R. LEENES, S. DE CONCA, *Artificial intelligence and privacy: AI enters the house through the cloud*, in W. Barfield, U. Pagallo (eds.), *Research handbook on the law of artificial intelligence*, Edward Elgar, Cheltenham, 2018, pp. 281 ss., i quali evidenziano l'ampio spazio di manovra dei titolari nella definizione degli scopi dei sistemi domestici intelligenti; sulla possibile qualificazione dell'utilizzatore finale quale titolare del trattamento dei dati raccolti attraverso il proprio sistema, si veda anche: EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *New Technologies Formation, Liability for Artificial Intelligence and Other Emerging Digital Technologies*, cit.

²⁵ EUROPEAN DATA PROTECTION BOARD, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adottata il 17 dicembre 2024: il Comitato precisa che i sistemi di intelligenza artificiale addestrati su dati personali non possono ritenersi anonimi in via generale, ma soltanto sulla base di una valutazione effettuata caso per caso; e sottolinea inoltre che il legittimo interesse può rappresentare una base giuridica del trattamento anche durante lo stadio di sviluppo dei modelli, a condizione che venga superato il test in tre fasi (legittimo interesse, necessità e bilanciamento), ribadendo così la vocazione del modello europeo a governare anche l'intelligenza artificiale generativa attraverso le ordinarie categorie del GDPR.

²⁶ Cfr. Garante per la protezione dei dati personali, provv. n. 755 del 2 novembre 2024, nei confronti di OpenAI, con imposizione di una sanzione amministrativa di 15 milioni di euro per violazioni relative alla base giuridica del trattamento, agli obblighi di trasparenza e alle procedure di verifica dell'età, comprendente anche l'ordine di promuovere una specifica campagna informativa: si tratta tra le prime decisioni sanzionatorie europee comminate al fornitore di un modello generativo ad ampia diffusione, come esito dell'istruttoria avviata dopo il blocco temporaneo del servizio imposto nel marzo 2023.

lizzabile in un'epoca in cui gli utenti comunicano enormi quantità di informazioni a terzi nel contesto delle attività ordinarie. Da quanto sopra scaturisce il dibattito sui correttivi da introdurre, che si divide tra chi suggerisce di qualificare i grandi operatori algoritmici come *information fiduciaries*, responsabili verso i propri utenti di doveri simili a quelli dell'avvocato o del medico²⁷, e chi propone di guardare al modello europeo. Quest'ultima direttrice ha già dato luogo a conseguenze normative. Il California Consumer Privacy Act, in vigore dal 2020 e potenziato dal California Privacy Rights Act, attribuisce al consumatore diritti di conoscenza, accesso, cancellazione e opposizione alla vendita dei dati, con divieto di discriminazione per il loro esercizio: un impianto normativo che guarda esplicitamente al GDPR, pur rimanendo, secondo la dottrina più attenta, una legge di trasparenza "all'americana", che guarda alla reazione del mercato prima ancora che alla tutela di principi indisponibili. L'orientamento californiano ha prodotto un'ondata imitativa che conta ad oggi circa venti legislazioni statali, mentre il Congresso non è riuscito nell'intento di approvare una legge federale generale²⁸. È il primo esempio di quell'andamento dinamico nella circolazione

Provvedimento successivamente annullato dal Tribunale di Roma con la sentenza n. 4153/2026, R.G. n. 4785/2025 del 18 marzo 2026.

²⁷ J. M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Ohio State Law Journal*, 2017, Vol. 78, pp. 1217 ss., il quale suggerisce di qualificare i grandi operatori algoritmici come *information fiduciaries*: similmente ai tradizionali fiduciari (come medici e avvocati), essi operano in una realtà contrassegnata da una elevata asimmetria di potere e informativa, nella quale gli utenti non hanno la possibilità di svolgere una efficace azione di controllo; da tutto ciò dovrebbero derivare, sia pure in una forma adattata al contesto digitale, doveri di lealtà (*duty of loyalty*) e di cura (*duty of care*) nei confronti di clienti ed *end-users*.

²⁸ Il California Consumer Privacy Act (Cal. Civ. Code, § 1798.100 ss.), in vigore dal 1° gennaio 2020, riconosce al consumatore il diritto di conoscere e accedere alle informazioni personali che sono state raccolte su di lui (§ 1798.110), il diritto alla cancellazione (§ 1798.105), il diritto di conoscere quali dati siano stati oggetto di condivisione e di vendita, ovvero comunicati per scopi commerciali e a quali categorie di destinatari (§ 1798.115), il diritto di opporsi alla condivisione o alla vendita dei dati (§ 1798.120) e il diritto di non subire discriminazioni per l'esercizio dei diritti che gli sono riconosciuti dalla legge (§ 1798.125). Il California Privacy Rights Act, approvato con referendum il 3 novembre 2020 e diventato operativo, nella sua componente principale, il 1° gennaio 2023, ne ha consolidato l'impianto ed ha istituito la California Privacy Protection Agency. In letteratura si veda: M. KAMINSKI, *A Recent Renaissance in Privacy Law*, in *ACM*, 2020, p. 24 ss.; nonché A. CHANDER, M. KAMINSKI, W. MCGEVERAN, *Catalyzing Privacy Law*, in *Minnesota Law*

dei modelli che verrà analizzato in dettaglio nei paragrafi che seguono. Prima di tale analisi, tuttavia, è necessario comprendere i motivi per cui l'intelligenza artificiale rende insufficiente una tutela costruita unicamente attorno all'individuo.

3. La dimensione collettiva della privacy nell'era dei *Big Data*: profilazione, *group privacy* e i limiti della tutela individuale

Intelligenza artificiale e *Big Data*, sul piano concettuale, non sono un binomio indistinguibile. La tecnologia informatica ha una lunga tradizione nello sviluppo di tecniche di apprendimento e rappresentazione, anche a prescindere dalla disponibilità di grandi quantità di dati, mentre solo più recentemente l'impiego di dati sintetici è salito al centro dell'attenzione anche con riferimento alla tutela della riservatezza²⁹; è ormai un fatto inconfutabile che le prestazioni dei sistemi tecnologici contemporanei tendano ad aumentare con la crescita delle informazioni disponibili, e che l'economia dell'intelligenza artificiale si alimenti di quella massa di dati che oggi viene descritta dalla formula delle “tre V”: volume, velocità, varietà³⁰. È da questo

Review, 2021, Vol. 105, p. 1734 ss., sulla funzione catalizzatrice della disciplina californiana. Tra le prime legislazioni organiche successive si possono segnalare il Virginia Consumer Data Protection Act del 2021 e il Colorado Privacy Act del 2021.

²⁹ In merito al graduale sviluppo di tecniche di apprendimento e di rappresentazione basate sull'elaborazione di esempi e sulla realizzazione dinamica di nuove *feature*, anziché sulla sola disponibilità di immense quantità di dati, si veda: G. PAGALLO, D. HAUSSLER, *Boolean Feature Discovery in Empirical Learning*, in *Machine Learning*, 1990, Vol. 5, pp. 71-99. Sulla rinnovata attenzione nei confronti dei dati sintetici anche come strumento di protezione della riservatezza, si veda: B. XIN ET AL., *Private FL-GAN: Differential Privacy Synthetic Data Generation Based on Federated Learning*, in *IEEE ICASSP*, 2020, p. 2927 ss., dove la generazione sintetica viene utilizzata per addestrare modelli limitando l'esposizione di dati personali reali.

³⁰ D. LANEY, *3D Data Management: Controlling Data Volume, Velocity and Variety*, in META Group Research Note, 2001, il quale introduce la tripartizione basata sulla velocità, sul volume e sulla varietà dei dati quali principali indicatori della crescente complessità del *data management*. Per un quadro generale delle tecnologie di apprendimento automatico collegate alla disponibilità di immense quantità di dati, si veda: E. ALPAYDIN, *Introduction to Machine Learning*, MIT Press, Cambridge (Mass.), 2014.

connubio di fatto, più che di necessità, che nasce il problema giuridico specificamente esaminato nel presente paragrafo.

Le tecniche di profilazione algoritmica non si basano su singoli individui, ma su ampi gruppi tipologici: aggregano le persone in classi create sulla base di predicati statistici, come ad esempio le abitudini di consumo, l'orientamento religioso, l'appartenenza etnica o la predisposizione a certe patologie, e su tali classi fondano le loro decisioni di inclusione od esclusione: da un servizio, da un prodotto, da un credito, da un'offerta di lavoro. Il singolo individuo viene raggiunto dagli effetti di tali decisioni in quanto appartenente ad un gruppo della cui stessa esistenza può essere ignaro³¹. A ciò si aggiungono i vizi epistemici che sono stati individuati dalla letteratura: evidenze inconcludenti che generano azioni ingiustificate, evidenze imperscrutabili che producono opacità, evidenze distorte che determinano discriminazioni³². Tutto ciò dà luogo ad una torsione del paradigma: una tutela interamente costruita in relazione all'individuo, al suo consenso e ai suoi diritti di accesso e cancellazione, stenta ad intercettare i pregiudizi che nascono e si consumano a livello aggregato³³.

³¹ U. PAGALLO, *The Group, the Private, and the Individual: A New Level of Data Protection?*, in L. Taylor, L. Floridi, B. van der Sloot (eds.), *Group Privacy: New Challenges of Data Technologies*, Springer, Dordrecht, 2017, p. 159 ss., il quale rileva che le tecniche di *data mining* e profilazione non agiscono sugli individui, ma su tipologie (*types*) realizzate attraverso principi classificatori, e a causa di ciò le decisioni algoritmiche possono incidere su un singolo individuo in quanto membro di un gruppo creato dalla tecnologia stessa e della cui esistenza egli può essere totalmente all'oscuro. Da ciò deriva la limitata efficacia di una modalità di protezione dei dati basata esclusivamente sulla relazione bilaterale tra l'interessato e il titolare del trattamento.

³² La tassonomia dei vizi epistemici degli algoritmi (*inconclusive evidence, inscrutable evidence e misguided evidence*) viene proposta da B. D. MITTELSTADT, P. ALLO, M. TADDEO, S. WACHTER, L. FLORIDI, *The Ethics of Algorithms: Mapping the Debate*, in *Big Data & Society*, 2016, Vol. 3, No. 2, pp. 4 ss., i quali distinguono le evidenze statisticamente incerte, quelle non intelligibili o verificabili e quelle distorte da *bias* nei dati o nei modelli, dimostrando che tali difetti possono dare luogo a esiti discriminatori. Sul piano empirico, C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown, New York, 2016, documenta l'effettiva incidenza di tali dinamiche nei settori del lavoro, dell'istruzione, del credito e della giustizia, descrivendo gli algoritmi come opachi, scalabili e quali possibili «armi di distruzione matematica».

³³ A. MANTELERO, *Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection*, in *Computer Law & Security Review*, 2016, Vol. 32, No. 2, pp. 238-255, il quale osserva che la tradizionale architettura

Anche in questo ambito, comunque, i due modelli sono divergenti tra loro. Nell'ordinamento statunitense la dimensione collettiva della privacy è stata ricondotta alla libertà di associazione prevista dal Primo Emendamento: dopo la sentenza della Corte Suprema in *Boy Scouts of America v. Dale*, la privacy del gruppo può essere concepita come diritto di un titolare unitario simile all'individuo; una privacy corporativa, quindi, di cui il caso citato rivela però il lato oscuro, perché fu la stessa associazione ad invocare la propria autonomia contro un proprio membro³⁴. Nell'ordinamento europeo, invece, le ipotesi di privacy associativa vengono interpretate alla luce della libertà di associazione e del divieto di discriminazione, ai sensi degli artt. 12 e 21 della Carta dei diritti fondamentali dell'Unione europea, mentre la tutela dei dati rimane legata alla persona fisica: il gruppo può agire, ma solo come strumento che rappresenta l'individuo, non come titolare di un diritto proprio; è la logica della rappresentanza di cui all'art. 80 GDPR. Ed è significativo che la Corte europea dei diritti dell'uomo, nella controversia *Big Brother Watch*, abbia riconosciuto come le organizzazioni siano legittimate quali titolari di diritti propri, non come portatrici di una *group privacy* dei soggetti profilati³⁵.

tura della protezione dei dati, costruita attorno al titolare del dato e ai suoi diritti individuali, sta mostrando limiti evidenti di fronte ai meccanismi di profilazione algoritmica, nei quali le decisioni vengono prese sulla base di *cluster* e gruppi di individui. Da ciò consegue l'esigenza di affiancare alla tutela individuale una *collective dimension of data protection*, idonea a prevenire i pregiudizi e le discriminazioni che danneggiano interessi collettivi e non solo individuali.

³⁴ Cfr. *Boy Scouts of America v. Dale*, 530 U.S. 640 (2000), dove la Corte Suprema, valorizzando la dottrina della *expressive association* desunta dal Primo Emendamento, ha riconosciuto all'associazione il diritto di escludere un assistente capo scout esplicitamente omosessuale, ritenendo che la sua presenza avrebbe esercitato una negativa incidenza sull'immagine pubblica dell'associazione. Tale pronuncia rappresenta uno dei più significativi precedenti da cui la dottrina desume il concetto di una tutela unitaria dell'identità e dell'autonomia del gruppo, assimilabile ad una forma di "privacy corporativa", ma pone in evidenza altresì il possibile conflitto tra l'autonomia collettiva e i diritti del singolo associato. Sul differente bilanciamento tra privacy e libertà di espressione nell'ordinamento europeo rispetto a quello statunitense, con particolare riferimento all'espansione del diritto all'oblio e alla sua proiezione extraterritoriale, si veda: D. C. NUNZIATO, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten*, in *University of Pennsylvania Journal of International Law*, 2018, Vol. 39, pp. 101 ss.

³⁵ Nell'ordinamento europeo, la dimensione collettiva della protezione dei dati viene riconosciuta soprattutto a livello procedurale. L'art. 80 GDPR legittima organismi, organizzazioni o associazioni senza scopo di lucro che perseguano finalità di interesse pub-

La riflessione teorica ha colto la tensione. Una componente autorevole della dottrina ha suggerito di prendere sul serio la *group privacy*, considerando come titolare del diritto il gruppo e non disgiuntamente i suoi membri³⁶. La proposta ha il merito di evidenziare il problema, ma presta il fianco a una critica importante: i diritti corporativi servono sovente a proteggere il gruppo contro alcuni dei suoi membri, ma rischiano di affidare agli enti e alle organizzazioni il potere decisionale sulla circolazione dei dati anche in antitesi alla volontà degli interessati, moltiplicando senza motivazioni plausibili le ipotesi, già previste in via straordinaria dall'art. 6, par. 1, lett. b)-f), GDPR, nelle quali il trattamento viene effettuato a prescindere dal consenso individuale³⁷. La dottrina italiana ha proposto, invece, una soluzione intermedia: una soluzione che non prevede un nuovo soggetto titolare, bensì una dimensione collettiva della tutela, basata su valutazioni di impatto etico-

blico ad esercitare per conto dell'interessato, ovvero, ove previsto dal diritto nazionale, anche indipendentemente da un mandato, i rimedi contemplati dal regolamento, senza attribuire tuttavia al gruppo la titolarità di un autonomo diritto relativo alla protezione dei dati. Cfr. Corte EDU, *Big Brother Watch e altri c. Regno Unito*, ric. nn. 58170/13, 62322/14 e 24960/15, Grande Camera, 25 maggio 2021, nella quale la Corte ha preso in esame i ricorsi promossi anche da organizzazioni della società civile contro i programmi di sorveglianza di massa, mantenendo tuttavia ancorata la tutela convenzionale agli artt. 8 e 10 CEDU quali diritti fondamentali delle persone fisiche, e non di un gruppo considerato quale autonomo titolare di situazioni soggettive.

³⁶ L. FLORIDI, *Open Data, Data Protection, and Group Privacy*, in *Philosophy & Technology*, 2014, Vol. 27, pp. 1-3, il quale sostiene che, rispetto ad alcune minacce informazionali, «*privacy as a group right is a right held by a group as a group rather than by its members severally*», è il gruppo in quanto tale, e non disgiuntamente i suoi membri, a dover essere identificato quale titolare del diritto. In una prospettiva convergente, B. VAN DER SLOOT, *Privacy in the Post-NSA Era: Time for a Fundamental Revision?*, in *JIPI-TEC*, 2014, Vol. 5, No. 2, il quale pone in evidenza come i fenomeni di *Big Data* e *group profiling* mettano in crisi un modello di privacy incentrato esclusivamente sull'individuo e sul pregiudizio personale, delineando l'esigenza di un ripensamento delle tradizionali categorie.

³⁷ U. PAGALLO, *Algo-Rhythms and the Beat of the Legal Drum*, in *Philosophy & Technology*, 2018, Vol. 31, p. 507 ss., il quale segnala che la semplice sostituzione del titolare individuale con il gruppo attribuirebbe a enti e organizzazioni il potere di legittimare trattamenti anche contro la volontà dei loro componenti, decidendo se i dati condivisi possano essere raccolti, trasmessi o cancellati, e aumenterebbe così, senza motivato fondamento, le ipotesi di trattamento indipendenti dal consenso che il GDPR ammette solo in via tassativa.

sociale dei trattamenti su larga scala e dei presidi procedurali attivabili da enti esponenziali³⁸.

Quella che in passato era solo una prospettiva teorica è diventata nel 2026 in larga parte una norma di diritto positivo. La Corte di giustizia ha infatti stabilito che il calcolo automatizzato di un punteggio di affidabilità creditizia rappresenta, di per sé, una “decisione automatizzata”, ai sensi dell’art. 22 GDPR, quando i terzi attribuiscono a tale calcolo un rilievo determinante: in tal modo la tutela individuale viene estesa a monte, colpendo la profilazione nella sua fase generativa e non soltanto nel suo utilizzo finale³⁹. Il Digital Services Act ha vietato la pubblicità basata sulle profilazioni che si avvalgano di particolari categorie di dati e, in particolare, la pubblicità rivolta ai minori, imponendo alle grandi piattaforme la valutazione e mitigazione dei rischi sistemici: una categoria che considera dichiaratamente il gruppo, anzi la società nel suo complesso, quale unità di misura del possibile pregiudizio⁴⁰. E l’AI Act ha

³⁸ A. MANTELERO, *Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection*, cit., pp. 238 ss., il quale ipotizza una misura collettiva della protezione dei dati, basata su valutazioni d’impatto in grado di considerare anche le conseguenze etiche e sociali dei trattamenti su ampia scala. Per una prospettiva comparatistica, si veda: U. PAGALLO, *The Collective Dimensions of Privacy in the Information Era: A Comparative Law Approach*, in *Annuario di diritto comparato e di studi legislativi*, 2020, Vol. 11, il quale analizza gli strumenti con cui i differenti ordinamenti gestiscono la protezione degli interessi collettivi coinvolti dal trattamento dei dati, mettendo in evidenza la necessaria centralità della persona fisica quale referente ultimo della tutela.

³⁹ Cfr. CGUE, 7 dicembre 2023, causa C-634/21, SCHUFA Holding (Scoring), punti 46-48 e 73-76: il calcolo automatizzato di un indice di probabilità relativo all’affidabilità creditizia di una persona rappresenta una valutazione fondata solo sul trattamento automatizzato ai sensi dell’art. 22 GDPR quando tale indice svolge una funzione determinante nella decisione del terzo di instaurare, eseguire o terminare un rapporto contrattuale con l’interessato. La Corte impedisce in tal modo che la tutela contemplata dall’art. 22 GDPR possa essere aggirata attraverso la frammentazione del processo decisionale tra il soggetto che calcola il punteggio e il soggetto che lo utilizza. La Corte ha poi chiarito che l’interessato ha il diritto di ricevere spiegazioni in merito alla procedura e in ordine ai principi applicati per giungere alla decisione automatica, in tal modo da poterla comprendere e contestare. Cfr. CGUE sentenza del 27 febbraio 2025 (causa C-203/22, Dun & Bradstreet Austria).

⁴⁰ Regolamento (UE) 2022/2065 (Digital Services Act): l’art. 26, par. 3, vieta alle piattaforme online di proporre pubblicità basata sulla profilazione attraverso l’utilizzo delle particolari categorie di dati di cui all’art. 9 GDPR; l’art. 28, par. 2, vieta la pubblicità rivolta ai minori basata sulla profilazione. Gli artt. 34 e 35 prescrivono alle piattaforme online di grandi dimensioni (VLOPs) e ai motori di ricerca online di grandi dimensioni (VLOSEs) di individuare, valutare e mitigare i rischi sistemici che derivano dai propri

vietato, a sua volta, le pratiche generalizzate di *social scoring* e l'identificazione delle emozioni nei luoghi di istruzione e di lavoro: un divieto che non presuppone nessuna comprovata lesione individuale, ma che neutralizza *ex ante* utilizzi tecnologici ritenuti incompatibili con i diritti fondamentali⁴¹. Il legislatore europeo, dunque, ha dato una risposta alla dimensione collettiva del rischio algoritmico non già attraverso la creazione di nuovi titolari, ma spostando gli effetti della tutela dal rimedio individuale alla regola preventiva.

Rimane, tuttavia, una lacuna. Le regole preventive salvaguardano il momento fisiologico; ma quando il pregiudizio si è ormai realizzato, ed è, come di solito accade, individualmente piccolo ma ingente nel suo complesso, la tutela individuale si rivela antieconomica, perché nessun interessato che abbia una visione razionale affronta i rischi di un giudizio per rivendicare il valore dei propri dati. Si tratta del medesimo problema con cui il diritto dei consumatori si confronta da un secolo, e che ha risolto attraverso lo strumento delle azioni collettive: la convergenza tra i due sistemi normativi, ai quali è dedicato il seguente paragrafo, ha origine da qui.

4. La convergenza con il diritto dei consumatori: azioni di classe, tra-pianti giuridici e l'esperienza italiana (dal caso *Facebook–AGCM a Meta c. Bundeskartellamt*)

Il diritto dei consumatori si confronta con la dimensione collettiva del pregiudizio eventuale. In un'economia caratterizzata dalla produzione e co-

servizi, con particolare riferimento agli effetti negativi che potrebbero prodursi sull'esercizio dei diritti fondamentali, sulla tutela dei minori, sul dibattito civico e sui processi democratici: la valutazione si sposta, in tal modo, dal pregiudizio individuale agli effetti sistemici prodotti sul complesso degli utenti e sulla società.

⁴¹ Regolamento (UE) 2024/1689 (AI Act), art. 5, par. 1, lett. c) e f): tra le pratiche di intelligenza artificiale che sono oggetto di divieto si annoverano i sistemi di *social scoring* che valutano o classificano le persone fisiche in relazione al comportamento sociale o alle caratteristiche personali o della personalità, quando possano produrre un trattamento pregiudizievole o sfavorevole in contesti sociali estranei a quelli nei quali i dati sono stati originariamente generati, ovvero sproporzionato rispetto al comportamento considerato, nonché gli *emotion recognition systems* utilizzati nei luoghi di lavoro e negli istituti di istruzione, salvo che per finalità di sicurezza o di carattere medico.

municazione di massa è inevitabile che numerose persone vengano danneggiate in maniera pressoché identica da prodotti di carattere seriale o da pratiche commerciali standardizzate; ed è altrettanto inevitabile che l'asimmetria informativa e di potere tra il gestore professionale e il consumatore generi rivendicazioni individualmente troppo esigue per giustificare una lite giudiziale. La risposta storica a tale scenario è l'azione di classe: un'azione associativa nella quale un componente del gruppo agisce in rappresentanza di tutti gli altri, tutelando in via giudiziale anche i diritti di chi ignora di essere stato danneggiato, e assolvendo così a una duplice funzione, deterrente e compensativa⁴². Non è difficile cogliere l'analogia con il pregiudizio algoritmico descritto nel paragrafo che precede: anche in quel caso il danno è opaco, seriale e individualmente esiguo; non a caso la dottrina statunitense ha ritenuto che la *class action* fosse lo strumento in grado di "tagliare il nodo gordiano" della responsabilità nell'*Internet of Things*⁴³.

Se la *class action* ha avuto origine e si è sviluppata nell'ambito del diritto statunitense, la sua diffusione negli ordinamenti di *civil law* rappresenta un capitolo esemplare di quella circolazione dei modelli giuridici studiata dal diritto comparato attraverso le categorie della ricezione e del trapianto: le regole migrano da un ordinamento all'altro con una frequenza molto maggiore rispetto alla loro creazione, e il loro radicamento dipende dal contesto culturale, professionale e istituzionale in cui vengono integrate⁴⁴. Non tutti gli in-

⁴² J. C. ALEXANDER, *An Introduction to Class Action Procedure in the United States, relazione alla conferenza Debates over Group Litigation in Comparative Perspective*, Ginevra, 2000, dove si rileva che, in un sistema caratterizzato dall'interdipendenza economica e dalla produzione e commercializzazione di massa, è fisiologico che una pluralità di individui subisca forme di pregiudizio che derivano da prodotti seriali o pratiche commerciali standardizzate; le *class actions* permettono di aggregare rivendicazioni individualmente troppo modeste per giustificare i costi di un processo, perseguendo congiuntamente gli obiettivi della deterrenza e della compensazione.

⁴³ D. ROBINSON, *Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation*, in *Richmond Journal of Law & Technology*, 2020, Vol. 26, No. 1, pp. 2-19, il quale propone la *class action* come prioritario strumento di protezione rispetto ai rischi sistemici che derivano dall'*Internet of Things*, sostenendo che la *litigation* collettiva possa riallineare gli incentivi dei produttori e sopperire all'inerzia regolatoria, agevolando l'adozione di standard di sicurezza più elevati.

⁴⁴ A. WATSON, *Legal Transplants: An Approach to Comparative Law*, University of Georgia Press, Athens, 1993, per il quale il trapianto di regole da un ordinamento

nesti hanno esito positivo; e quando ciò accade, raramente l'istituto trapiantato rimane uguale a sé stesso⁴⁵. L'esperienza italiana può definirsi, in tal senso, un laboratorio ideale, presentando tre episodi dagli esiti opposti.

Il primo episodio si riferisce a un trapianto riuscito: ossia la disciplina dei dati personali. La direttiva 95/46/CE trovò attuazione con la legge del 31 dicembre 1996 n. 675, e le successive stratificazioni europee vennero via via recepite senza alcuna crisi di rigetto, fino alla diretta applicabilità del GDPR; il segno più evidente di tale successo è di natura linguistica, perché, a partire dalla metà degli anni Novanta, la parola "privacy" è entrata stabilmente a far parte del lessico italiano, sia nel linguaggio giuridico che nell'idioma comune⁴⁶. Il secondo episodio mostra invece una crisi di rigetto: il codice di procedura penale del 1988 tentò di sostituire il sistema inquisitorio con un mo-

all'altro rappresenta il più importante motore dell'evoluzione giuridica, molto più della creazione originaria. Nella letteratura italiana si veda: R. SACCO, *Introduzione al diritto comparato*, UTET, Torino, 1992, il quale sottolinea che la circolazione dei modelli dipende dalle modalità con le quali i diversi formanti dell'ordinamento ricevente reinterpretano la regola importata. Nella dottrina italiana, si veda: U. MATTEI, *Efficiency in Legal Transplants: An Essay in Comparative Law and Economics*, in *International Review of Law and Economics*, 1994, pp. 3 ss. In una prospettiva critica, si veda: P. LEGRAND, *The Impossibility of "Legal Transplants"*, in *Maastricht Journal of European and Comparative Law*, 4, 1997, pp. 111-124, il quale afferma che il senso delle regole è inscindibile dalla cultura giuridica dell'ordinamento in cui tali regole agiscono, per cui ciò che circola non è la regola in quanto tale, ma il suo testo, inevitabilmente riletto e modificato dal contesto ricevente.

⁴⁵ M. GRAZIADEI, *Comparative Law as the Study of Transplants and Receptions*, in M. Reimann, R. Zimmermann (eds.), *The Oxford Handbook of Comparative Law*, Oxford University Press, Oxford, 2019, pp. 442 ss., spec. pp. 461-463, il quale evidenzia che la ricezione non consiste mai in una meccanica riproduzione del modello straniero: il diritto importato è fatto oggetto di un processo di adattamento, appropriazione e reinterpretazione da parte dell'ordinamento ricevente, per cui lo studio dei trapianti giuridici si identifica, in realtà, con lo studio dei processi di revisione del modello trasferito.

⁴⁶ La direttiva 95/46/CE venne attuata con la legge 31 dicembre 1996, n. 675; il percorso di europeizzazione della disciplina è poi continuato con il d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), successivamente adeguato al regolamento (UE) 2016/679 con il d.lgs. 10 agosto 2018, n. 101, fino alla diretta applicazione del GDPR. In relazione all'ingresso della parola "privacy" nel lessico giuridico e nel linguaggio comune italiano quale indice del successo della ricezione del modello europeo, si veda: U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, cit., il quale spiega che il neologismo è ormai entrato stabilmente nell'uso corrente, pur essendo perlopiù pronunciato «all'americana» anziché «all'inglese».

dello accusatorio mutuato dal contesto angloamericano, ma alcune disposizioni cardine della riforma entrarono in contrasto con i principi costituzionali vigenti a quel tempo, per cui la Corte costituzionale ne ridimensionò l'impianto con le note pronunce del 1992; fu necessaria una revisione costituzionale, il "giusto processo" previsto dall'art. 111 Cost., perché l'innesto potesse essere riproposto su basi finalmente compatibili⁴⁷.

Il terzo episodio concerne l'azione di classe. Il confronto parlamentare sull'importazione del modello statunitense iniziò nel 2004 e approdò, con la legge finanziaria del 2008, all'art. 140-bis del codice del consumo, in vigore, dopo rinvii e riscritture, dal 1° gennaio 2010, che prevedeva un'azione risarcitoria collettiva limitata tuttavia ai rapporti di consumo⁴⁸. Tale disciplina è stata successivamente superata: infatti la legge del 12 aprile 2019 n. 31 ha trasferito tale istituto nel codice di procedura civile (artt. 840-bis ss. c.p.c.), affrancandolo dalla matrice consumeristica e dotandolo di modalità di adesione anche successive alla sentenza, per cui è oggi legittimato ad agire, oltre alle organizzazioni iscritte in un apposito elenco, chiunque avanzi pretese omogenee⁴⁹. Nel contesto europeo, la direttiva (UE) 2020/1828 relativa alle

⁴⁷ Il codice di procedura penale approvato con D.P.R. 22 settembre 1988, n. 447 puntò a sostituire il sistema inquisitorio con un modello accusatorio di ispirazione anglosassone; la Corte costituzionale ne ridimensionò l'impianto originario con le sentenze nn. 24, 254 e 255 del 1992, dando risalto al principio di non dispersione della prova. La riforma dell'art. 111 Cost., introdotta dalla legge costituzionale 23 novembre 1999, n. 2, ha successivamente costituzionalizzato i principi del giusto processo e del contraddittorio nella formazione della prova, permettendo il consolidamento del modello accusatorio su basi costituzionali compatibili.

⁴⁸ L'art. 140-bis cod. cons. venne introdotto dall'art. 2, comma 446, della legge 24 dicembre 2007, n. 244, e riscritto dall'art. 49 della legge 23 luglio 2009, n. 99, entrando in vigore il 1° gennaio 2010: sei anni di discussioni e lavori, avviati dal confronto parlamentare del 2004, sull'opportunità di importare il modello statunitense nel codice del consumo italiano.

⁴⁹ La legge 12 aprile 2019, n. 31 ha modificato la disciplina dell'art. 140-bis cod. cons., trasferendo l'azione di classe negli artt. 840-bis ss. c.p.c.; dopo due differimenti, la nuova disciplina viene applicata alle condotte illecite successive al 19 maggio 2021. L'azione può essere oggi esperita da ogni titolare di diritti individuali omogenei, nonché dalle organizzazioni e associazioni iscritte all'elenco tenuto presso il Ministero della Giustizia, anche al di fuori dei rapporti di consumo, e prevede una modalità di adesione esercitabile anche successivamente alla sentenza di accoglimento. L'evoluzione dell'istituto rappresenta un significativo esempio di trapianto giuridico progressivamente rimodellato dall'ordinamento italiano in base al proprio assetto processuale.

azioni rappresentative, attuata in Italia con il d.lgs. 10 marzo 2023 n. 28 (artt. 140-ter ss. cod. cons.), ha compiuto il passo risolutivo relativamente alla definizione della materia di cui si tratta: tra le normative la cui violazione legittima l'azione rappresentativa figura esplicitamente il GDPR, per cui la saldatura tra la protezione collettiva di carattere consumeristico e la tutela dei dati non è più una proposta meramente dottrinale, ma diviene diritto positivo dell'Unione europea⁵⁰.

L'esperienza italiana aveva comunque dimostrato, in via giurisprudenziale, che i due sistemi normativi erano complementari, e non alternativi, prima ancora che ciò fosse codificato dal legislatore europeo. Il riferimento in tal senso è la vicenda *Facebook-AGCM*. Nel novembre 2018 l'Autorità garante della concorrenza e del mercato sanzionò Facebook Inc. e Facebook Ireland per complessivi dieci milioni di euro, contestando due distinte pratiche commerciali ritenute scorrette: una pratica ingannevole, consistente nell'accompagnare la registrazione alla piattaforma con il famoso *claim* "Iscriviti. È gratis e lo sarà per sempre", senza informare in modo chiaro l'utente che i suoi dati sarebbero stati raccolti e utilizzati per finalità commerciali, e una pratica aggressiva, concernente il meccanismo di trasferimento dei dati a terzi⁵¹. Facebook si difese affermando, tra l'altro, che il ser-

⁵⁰ Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori, attuata in Italia con il d.lgs. 10 marzo 2023, n. 28, che ha introdotto gli artt. 140-ter ss. cod. cons.: l'allegato I della direttiva ricomprende espressamente il regolamento (UE) 2016/679 (GDPR) tra gli atti dell'Unione la cui violazione può essere fatta valere attraverso azioni rappresentative nazionali e transfrontaliere, creando un esplicito legame, sul piano del diritto positivo, fra gli strumenti di tutela collettiva dei consumatori e la disciplina della protezione dei dati personali, in sintonia con il sistema di rappresentanza previsto dall'art. 80 GDPR.

⁵¹ Cfr. *AGCM, provvedimento 29 novembre 2018, n. 27432* (procedimento PS11112), avviato il 6 aprile 2018 anche in seguito alle segnalazioni pervenute da associazioni di consumatori, che ha verificato la violazione degli artt. 20, 21, 22, 24 e 25 cod. cons., irrogando due sanzioni amministrative pecuniarie di euro 5.000.000 ciascuna: la prima per la pratica commerciale ingannevole consistente nel presentare il servizio come gratuito («Iscriviti. È gratis e lo sarà per sempre») senza fornire una chiara informativa in merito alla raccolta e allo sfruttamento commerciale dei dati personali; la seconda per la pratica commerciale aggressiva consistente nell'indurre gli utenti, mediante strumenti di preselezione delle impostazioni, a permettere la comunicazione dei propri dati a siti web e applicazioni di terzi per finalità di natura commerciale.

vizio era veramente gratuito e che ogni problematica concernente l'utilizzo dei dati era di pertinenza esclusiva del Garante privacy, non dell'AGCM. Il TAR del Lazio respinse tale difesa obiettando che il servizio non era gratuito, poiché oltre alla protezione del dato personale come espressione di un diritto della personalità, garantito da tutele irrinunciabili quali la revoca del consenso, l'accesso, la rettifica, l'oblio, vi è un distinto ambito di tutela del dato come possibile oggetto di scambio, e tale "patrimonializzazione" del dato impone agli operatori del settore i medesimi obblighi di chiarezza e completezza informativa che appartengono alla normativa consumeristica; su tali basi il giudice amministrativo confermò la sanzione per la pratica ingannevole, annullando invece la sanzione per la pratica aggressiva⁵². E il Consiglio di Stato confermò tale impostazione: la disciplina della protezione dei dati non deve considerarsi un microcosmo autosufficiente che dispensa dall'applicazione del codice del consumo, perché le due normative, l'una finalizzata a garantire l'autodeterminazione informativa della persona, l'altra volta a tutelare la libertà di autodeterminazione economica del consumatore, hanno ambiti e scopi che sono tra loro diversi e complementari⁵³.

⁵² TAR Lazio, sez. I, 10 gennaio 2020, nn. 260 e 261, che hanno respinto l'eccezione di incompetenza dell'AGCM sostenendo che, accanto alla protezione del dato personale come fondamentale diritto della persona, confermato dalle garanzie che sono proprie della disciplina in materia di protezione dei dati, esiste un diverso profilo riguardante il valore economico del dato come possibile bene di scambio nelle relazioni di mercato, rispetto al quale devono applicarsi gli obblighi di trasparenza, chiarezza e non ingannevolezza previsti dal codice del consumo. Il TAR ha quindi convalidato la sanzione relativa alla pratica commerciale ingannevole, mentre ha annullato la sanzione relativa alla pratica commerciale aggressiva, ritenendo non sufficientemente dimostrata la sussistenza degli elementi costitutivi di quest'ultima.

⁵³ Cons. Stato, sez. VI, 29 marzo 2021, nn. 2630 e 2631, che hanno respinto sia l'appello di Facebook sia quello incidentale dell'AGCM, confermando il punto di vista del TAR Lazio. Il Consiglio di Stato ha sostenuto che la disciplina del GDPR non ha carattere esclusivo né assorbente, perché ritenere applicabile ai dati personali il solo regolamento europeo porterebbe a risultati irragionevoli, in quanto i dati personali sono coinvolti nella quasi totalità delle attività del sistema economico. La protezione dei dati personali e quella assicurata dal codice del consumo hanno finalità diverse e complementari: la prima assicura la liceità del trattamento e l'autodeterminazione informativa dell'interessato; la seconda detta obblighi di correttezza e trasparenza in ordine al valore economico dei dati e ai fini commerciali del loro utilizzo.

La suddetta vicenda apre al comparatista un campo di riflessione concettuale prima ancora che pratico: vale a dire la coesistenza, nello stesso ordinamento, di una tutela indisponibile del dato quale attributo della persona e quale tutela negoziale. La tensione tra l'idea che "noi siamo i nostri dati" e l'idea che "noi possediamo i nostri dati" non deve intendersi come una contrapposizione da risolvere, ma come una complementarità da governare⁵⁴. E i successivi sviluppi del diritto europeo hanno ratificato entrambi gli aspetti di tale ragionamento. Da un lato, la direttiva (UE) 2019/770 ha esplicitamente ampliato le garanzie contrattuali del consumatore includendo quei contratti dove il consumatore non paga un corrispettivo economico ma fornisce dati personali, ammettendo così sul piano normativo ciò che il giudice italiano aveva affermato sul piano rimediale⁵⁵. Dall'altro lato, la Corte di giustizia europea, nella vicenda *Meta Platforms c. Bundeskartellamt*, ha stabilito che un'autorità di vigilanza sulla concorrenza può accertare, quale elemento attestante un abuso di posizione dominante, la non conformità al GDPR del trattamento dei dati praticato da un'impresa, salvo il dovere di cooperazione leale con le autorità di protezione dei dati. La convergenza tra la protezione dei dati, il diritto dei consumatori e il diritto della concorrenza, sperimentata in Italia nel confronto tra l'AGCM e il giudice amministrativo, rappresenta

⁵⁴ U. PAGALLO, *Data Protection in EU and US Laws and AI: What Legal Changes We Should Expect in the Foreseeable Future?*, cit., pp. 602-605 e 613, il quale identifica nella coesistenza della concezione personalistica della tutela dei dati, propria dell'ordinamento europeo e dell'approccio proprietario statunitense, uno dei più rilevanti nodi teorici che verranno accentuati dallo sviluppo dell'intelligenza artificiale. Per l'inquadramento civilistico dello scambio fra servizi digitali e dati personali nella dottrina italiana, si veda: G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, pp. 416-420, dove gli autori mostrano come, nei servizi all'apparenza "gratuiti", il consenso al trattamento svolga anche una funzione economica, ponendosi in un rapporto sinallagmatico che mette in tensione la teoria del contratto e l'indisponibilità dei diritti della personalità.

⁵⁵ Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuti e servizi digitali, il cui art. 3, par. 1, ne estende l'ambito di applicazione anche ai contratti nei quali il consumatore, anziché pagare un prezzo, fornisce o si impegna a fornire dati personali al professionista, fatti salvi i casi in cui tali dati siano trattati esclusivamente per la fornitura del contenuto o del servizio digitale, ovvero per adempiere obblighi di legge. La direttiva è stata attuata in Italia con il d.lgs. 4 novembre 2021, n. 173, che ha istituito gli artt. 135-octies-135-vicies ter del codice del consumo.

un'anticipazione rilevante nel diritto dell'Unione europea⁵⁶. Il trapianto, in sostanza, ha seguito due distinti itinerari: dall'America all'Italia per quanto concerne lo strumento collettivo e consumeristico, e dall'esperienza applicativa italiana al diritto europeo quale anticipazione e sviluppo parallelo. C'è da domandarsi se tale tutela, seppure potenziata sul versante rimediabile, sia effettivamente sufficiente di fronte a tecnologie che possono produrre il rischio più rapidamente di quanto il rimedio sia in grado di accertarlo: ed è questa la domanda alla quale si cercherà di rispondere nell'ultimo paragrafo della presente riflessione.

5. Dal rimedio alla prevenzione: l'approccio proattivo europeo, l'AI Act e il Digital Omnibus. Considerazioni conclusive

La differenza più profonda tra i due modelli, quello europeo e quello statunitense, non consiste, in realtà, né nello statuto del dato né nel perimetro della regolazione, bensì nella struttura delle tutele. Nell'ordinamento statunitense il dato viene trattato soprattutto come bene di scambio, e le tutele, anche per le informazioni personali identificabili, operano con modalità rimediali: intervengono cioè dopo il danno, e delegano la funzione preventiva all'effetto di deterrenza dei rimedi e delle azioni di classe quale pratica di controllo degli incidenti, in base a una grammatica che la teoria del diritto ha reso familiare in relazione alla responsabilità civile⁵⁷. Il diritto europeo si ba-

⁵⁶ CGUE, Grande Sezione, 4 luglio 2023, causa C-252/21, Meta Platforms Inc. e a. c. Bundeskartellamt: la Corte ha sostenuto che, durante l'accertamento di un abuso di posizione dominante, un'autorità nazionale garante della concorrenza può esaminare e, qualora sia necessario ai fini dell'applicazione dell'art. 102 TFUE, accertare incidentalmente la conformità di un trattamento di dati personali al GDPR, fermo rimanendo l'obbligo di cooperazione leale con la competente autorità di controllo ai sensi del regolamento. La Corte ha inoltre affermato che la personalizzazione della pubblicità non rende, di per sé, il trattamento dei dati necessario all'esecuzione del contratto ai sensi dell'art. 6, par. 1, lett. b), GDPR, e che il consenso dato a una società in posizione dominante, pur non potendosi escludere in via assoluta, richiede una rigorosa verifica della sua libertà effettiva ai sensi dell'art. 6, par. 1, lett. a), GDPR.

⁵⁷ Il paradigma economico della responsabilità civile quale tecnica atta a prevenire gli incidenti trova la sua classica formulazione in G. CALABRESI, *The Costs of Accidents*. A

sa sul principio opposto, ossia che il trattamento dei dati è, di per sé, un'attività rischiosa, da governare prima che il rischio si trasformi in danno. Il termine “rischio” ricorre infatti più volte nel GDPR, il cui impianto è stato correttamente definito come una combinazione di regole di gestione, di valutazione e di governo del rischio; e l'art. 35, prescrivendo la valutazione d'impatto preventiva per i trattamenti ad elevato rischio basati sulle nuove tecnologie, offre il fondamento giuridico sul quale poggia oggi la dottrina per confrontarsi con le applicazioni dell'intelligenza artificiale⁵⁸. La stessa protezione dei dati fin dalla progettazione, oggi codificata dall'art. 25, scaturisce dall'idea che la protezione debba operare prima ancora che venga raccolto un solo *bit*, incorporandosi nell'architettura sistemica del software⁵⁹.

Proattività, peraltro, non vuol dire soltanto comando verticale. L'esperienza comparata conosce modalità preventive sperimentali e co-regolate: dalle zone speciali create dal governo giapponese fin dall'inizio degli anni Duemila al fine di testare in via preventiva le sfide giuridiche poste dalla robotica e dall'intelligenza artificiale, fino agli spazi di sperimentazione normativa che l'AI Act ha ora codificato, imponendo ad ogni Stato dell'Unione europea la creazione di *sandbox* regolatorie⁶⁰. Ed è importante rilevare che, sul piano

Legal and Economic Analysis, Yale University Press, New Haven, 1970, dove la responsabilità civile viene considerata uno strumento per minimizzare il costo sociale degli incidenti attraverso efficienti incentivi alla prevenzione.

⁵⁸ Il computo delle molteplici occorrenze del termine *risk* e la lettura del GDPR come insieme di regole di *risk management* (art. 5, par. 2), *risk assessment* (art. 24) e *risk governance* (art. 55) si devono a U. PAGALLO, *Data Protection in EU and US Laws and AI: What Legal Changes We Should Expect in the Foreseeable Future?*, cit., p. 615, il quale spiega che il rischio rappresenta la categoria ispiratrice di tutto il modello europeo di tutela dei dati. Lo stesso autore evidenzia che l'art. 35 GDPR, attraverso l'obbligo della valutazione d'impatto preventiva «*where a type of processing, in particular using new technologies*», rappresenta il naturale fondamento applicativo anche per i trattamenti fondati sull'intelligenza artificiale. In tal senso, si veda anche: R. GELLERT, *The Risk-Based Approach to Data Protection*, Oxford University Press, Oxford, 2020.

⁵⁹ L'art. 25 GDPR disciplina la protezione dei dati a partire dalla progettazione e per impostazione predefinita; la genealogia di tale principio ha origine dall'elaborazione promossa, a cavallo degli anni Duemila, da Ann Cavoukian, a quel tempo Information and Privacy Commissioner dell'Ontario.

⁶⁰ Sulle *National Strategic Special Zones* giapponesi (*Tokku*), che vennero utilizzate fin dall'inizio degli anni Duemila come strumenti di sperimentazione regolatoria nei settori della robotica e successivamente dell'intelligenza artificiale, si veda: U. PAGALLO, *Legal-*

normativo, la proattività è diventata una priorità anche oltre Atlantico, dove la relazione finale della National Security Commission on Artificial Intelligence ha conferito ad essa un rilievo strategico⁶¹, nonostante la posizione federale, negli anni recenti, abbia optato per una visione maggiormente deregolatoria⁶².

Nel 2026 il sistema proattivo europeo ha assunto una fisionomia completa nelle sue linee portanti. L'AI Act ha generalizzato l'approccio basato sul rischio creando un ordine che va dal divieto assoluto delle pratiche inaccet-

IAIze: Tackling the Normative Challenges of Artificial Intelligence and Robotics through the Secondary Rules of Law, in M. Corrales, M. Fenwick, N. Forgó (eds.), *New Technology, Big Data and the Law*, Springer, Singapore, 2017, pp. 281-300, dove l'Autore interpreta tali esperienze come esempi di regolazione sperimentale basata sulle *secondary rules* del diritto. Sul fronte europeo, gli artt. 57-59 del Regolamento (UE) 2024/1689 (AI Act) disciplinano gli *AI regulatory sandboxes*, obbligando gli Stati membri a creare almeno uno spazio di sperimentazione normativa; il termine per l'istituzione è stato spostato ad agosto 2027 dal Regolamento (UE) 2026/1744 (AI Act/Digital Omnibus). In relazione alla disciplina delle *regulatory sandboxes* in un'ottica comparata, si vedano in letteratura: A. STAZI, R. JOVINE, *A Comparative Analysis of Regulatory Sandboxes: Models, Evolution and Strategic Implications in EU, USA and China*, in *Comparative Law Review*, 2025, Vol. 16, No. 2, pp. 22-66; e A. STAZI, R. JOVINE, *A Comparative Analysis of Regulatory Sandboxes: Models, Evolution and Strategic Implications in the UAE and Singapore*, in *Rivista di diritto dei media*, 2026, Vol. 1, pp. 2 ss.

⁶¹ Cfr. *National Security Commission on Artificial Intelligence, Final Report, 2021*, dove si sollecita lo Stato statunitense ad agire con immediatezza per riorganizzare le istituzioni, investire nell'innovazione, accelerare l'adozione dell'intelligenza artificiale e predisporre alle sfide strategiche della competizione tecnologica globale. La logica è quella di stimolare l'intervento pubblico in funzione della competitività economica e della sicurezza nazionale, più che della tutela dei diritti fondamentali.

⁶² L'Executive Order 14110 del 30 ottobre 2023 (*Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*) aveva impostato un organico intervento federale in materia di intelligenza artificiale, imponendo diversi adempimenti di *reporting*, valutazione dei rischi e coordinamento amministrativo. Esso tuttavia è stato revocato dall'Executive Order 14148 del 20 gennaio 2025, seguito dall'Executive Order 14179 del 23 gennaio 2025 (*Removing Barriers to American Leadership in Artificial Intelligence*), che ha nuovamente spinto la politica federale verso la promozione della competitività e dell'innovazione. Questo indirizzo è stato ulteriormente confermato dall'Executive Order 14365 dell'11 dicembre 2025 (*Ensuring a National Policy Framework for Artificial Intelligence*) e dal successivo *National Policy Framework for Artificial Intelligence* del marzo 2026, che prospettano un quadro federale uniforme finalizzato a limitare la frammentazione delle discipline statali e a promuovere la leadership statunitense nel settore dell'intelligenza artificiale. Tale evoluzione conferma che il sistema statunitense tende a privilegiare strumenti di promozione e coordinamento dell'innovazione piuttosto che una regolazione generale di tipo prescrittivo.

tabili ai vincoli di conformità per i sistemi a rischio elevato, fino agli obblighi di trasparenza per i sistemi a rischio limitato e alle regole relative ai modelli per finalità generali. Ma anche la colonna portante rimediale è stata rinnovata coerentemente con il modello: la nuova direttiva riguardante la responsabilità da prodotto difettoso ha esplicitamente ricompreso il software e i sistemi di intelligenza artificiale tra tali prodotti, ha ampliato il danno risarcibile alla cancellazione e corruzione dei dati, ha esteso la responsabilità del produttore anche all'apprendimento e agli aggiornamenti successivi all'immissione in commercio ed ha attenuato l'onere probatorio del danneggiato con presunzioni e obblighi di *disclosure*, dando una risposta, su ogni punto, alle insufficienze che la dottrina aveva rilevato nel regime del 1985 rispetto ai prodotti intangibili⁶³. L'Italia, da parte sua, ha affiancato alla legislazione europea una normativa nazionale di *governance* e una garanzia penale della persona rispetto ai contenuti generati in modo artificiale⁶⁴.

⁶³ Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativa alla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE, con termine di recepimento fissato al 9 dicembre 2026: il software, inclusi i sistemi di intelligenza artificiale, viene esplicitamente ricompreso nella nozione di prodotto; il danno risarcibile comprende la distruzione o la corruzione dei dati non utilizzati solamente per fini professionali; il produttore risponde anche dei difetti che derivano da aggiornamenti, mancati aggiornamenti di sicurezza e dall'evoluzione del software, incluse le funzionalità di apprendimento programmate dal progetto del prodotto. L'introduzione di ordini di esibizione dei fattori di prova e di presunzioni relative in materia di difettosità e nesso causale punta ad attenuare le difficoltà probatorie che derivano dalla complessità tecnica dei prodotti digitali. La proposta di direttiva sulla responsabilità extracontrattuale per l'intelligenza artificiale (*Artificial Intelligence Liability Directive – AILD*), presentata nel 2022, è stata esclusa dalla Commissione europea dal Programma di lavoro per l'anno 2025, con la conseguenza che la responsabilità extracontrattuale continua ad essere regolata dai regimi nazionali, integrati dalla nuova normativa europea sulla responsabilità da prodotto.

⁶⁴ Cfr. Legge 23 settembre 2025, n. 132, recante disposizioni e deleghe al Governo in materia di intelligenza artificiale: la legge affianca al quadro europeo una disciplina nazionale di *governance*, precisando le autorità competenti per l'attuazione dell'AI Act e coordinandone le funzioni, e interviene inoltre sulla protezione penale della persona inserendo nel codice penale il delitto di illecita diffusione di contenuti generati od alterati mediante l'intelligenza artificiale (art. 612-quater c.p.), al fine di rafforzare la tutela dell'identità personale e della dignità della persona rispetto ai contenuti realizzati con tecnologie digitali.

Il Digital Omnibus, approvato in via definitiva, ha rinviato di oltre un anno gli obblighi previsti per i sistemi ad alto rischio: un rinvio causato dal ritardo degli standard armonizzati e delle autorità nazionali; e tuttavia, nello stesso testo, ha aggiunto un divieto operativo contro i sistemi generativi di contenuti intimi non consensuali. Una lettura attenta può suggerire che non si tratta di una ritirata dal modello proattivo, ma di un'esigenza di manutenzione: infatti slittano solo gli adempimenti, ma non i divieti né la logica relativa ai fattori di rischio. Più complessa appare la problematica relativa alla semplificazione del GDPR, il cui negoziato registra attualmente una fase di attesa dopo che le autorità europee di protezione dei dati hanno avvertito i colegislatori sul rischio di ridurre, per via di "semplificazione", la definizione di dato personale: il problema non è il fattore calendario, ma l'identità personalistica del modello⁶⁵. Si tratta di tensioni che la dottrina aveva previsto, dividendosi fra chi aveva avvertito che un approccio interamente proattivo rischiava una rapida obsolescenza e frammentazione, richiedendo revisioni troppo frequenti per garantire stabilità e certezza⁶⁶, e chi, pur difenden-

⁶⁵ Regolamento (UE) 2026/1744 del Parlamento europeo e del Consiglio, dell'8 luglio 2026, che modifica il Regolamento (UE) 2024/1689 (AI Act), pubblicato nella GUUE del 24 luglio 2026 e in vigore dal 27 luglio 2026: l'applicazione degli obblighi per i sistemi di intelligenza artificiale ad alto rischio è differita al 2 dicembre 2027 (sistemi di cui all'art. 6, par. 2, e all'allegato III) e al 2 agosto 2028 (sistemi di cui all'art. 6, par. 1, e all'allegato I), a causa del ritardo nell'elaborazione degli standard armonizzati e nella designazione delle autorità competenti; il medesimo intervento ha tuttavia introdotto un divieto, applicabile dal 2 dicembre 2026, riguardante i sistemi finalizzati alla generazione di contenuti intimi sintetici non consensuali. La Commissione europea ha inoltre pubblicato, il 10 giugno 2026, un codice di buone pratiche sulla marcatura e l'etichettatura dei contenuti generati dall'intelligenza artificiale, a supporto degli obblighi di trasparenza previsti dall'art. 50 dell'AI Act. Per quanto riguarda il parallelo pacchetto di semplificazione del GDPR e della direttiva e-Privacy, il procedimento legislativo risultava ancora pendente alla metà del 2026, dopo che EDPB ed EDPS avevano manifestato riserve sulle proposte di modifica della nozione di dato personale, ritenendo che esse eccedessero una mera semplificazione tecnica e potessero condizionare il livello di tutela assicurato dal regolamento.

⁶⁶ In letteratura, si veda: U. PAGALLO, *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, in *European Data Protection Law Review*, 2017, Vol. 3, No. 1, pp. 39-43, il quale, a partire dalla distinzione hartiana tra norme primarie e norme secondarie, sostiene che una regolazione affidata solamente a norme sostanziali può frenare l'innovazione tecnologica o richiedere revisioni troppo frequenti per assicurare stabilità e certezza; da ciò deriva l'esigenza di strumenti di fles-

do l'impianto del legislatore europeo, ne aveva segnalato le ambiguità applicative⁶⁷.

La comparazione condotta approda a tre risultati. Il primo risultato è di carattere strutturale: il modello europeo e il modello statunitense sono divisi sia dallo statuto del dato, diritto della personalità nell'uno e *commodity* nell'altro, sia dalla logica delle tutele, l'una preventiva e l'altra rimediale. Ma la contrapposizione tra persona e mercato, che dà il titolo al presente contributo, attraversa dall'interno entrambi gli ordinamenti giuridici, come attestano da un lato la patrimonializzazione del dato nei contratti digitali, riconosciuta sia dal giudice italiano che dal legislatore europeo, e dall'altro lato l'importazione di diritti di origine europea nelle legislazioni statali statunitensi. Il secondo risultato è di carattere dinamico: l'intelligenza artificiale e la dimensione collettiva del pregiudizio algoritmico operano come elemento di convergenza, alimentando una circolazione dei modelli che si muove nei due sensi: dagli Stati Uniti verso l'Europa lo strumentario collettivo e consumeristico e dall'Europa verso gli Stati Uniti la grammatica dei diritti sull'informazione. Mentre l'esperienza italiana, dal riuscito trapianto della disciplina dei dati al caso Facebook–AGCM, mostra come un ordinamento ricevente possa non solo assimilare l'innesto, ma anticipare soluzioni che potranno poi essere generalizzate a livello europeo. Il terzo risultato è di natura prospettica: la scommessa distintiva del modello europeo, ossia gover-

sibilità, adattamento e coordinamento in grado di preservare la natura “*future-proof*” della disciplina.

⁶⁷ L. FLORIDI, *The European Legislation on AI: A Brief Analysis of Its Philosophical Approach*, in *Philosophy & Technology*, 2021, Vol. 34, pp. 215-222, spec. pp. 216-221, il quale considera in modo positivo l'impostazione filosofica dell'AI Act, apprezzandone l'orientamento volto a creare una disciplina basata sul rischio, sulla protezione dei diritti fondamentali e sulla regolazione degli utilizzi dell'intelligenza artificiale, pur mettendo in evidenza diverse ambiguità applicative e concettuali, relative, tra l'altro, alla nozione di sistemi ad alto rischio, alla tassonomia dei rischi e ad alcuni aspetti tecnici della disciplina. In posizione maggiormente critica, M. EBERS, V.R.S. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER, B. STEINRÖTTER, *The European Commission's Proposal for an Artificial Intelligence Act: A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, in *J*, 2021, Vol. 4, No. 4, pp. 589-603, spec. pp. 590-601, che elencano diverse criticità della proposta, riguardanti, fra l'altro, l'eccessiva ampiezza della definizione di intelligenza artificiale, la classificazione dei sistemi ad alto rischio, i meccanismi di *enforcement*, la standardizzazione e le carenze della disciplina.

nare il rischio tecnologico in anticipo sul danno, è entrata nella fase di prova, tra necessità di semplificazione, spinte competitive e manutenzioni normative che ne testano la tenuta, senza per il momento modificarne la logica.

Resta, alla fine, la domanda con cui si è aperto il presente lavoro: ossia se il diritto privato dei dati abbia la capacità di confrontarsi con tecnologie che apprendono, si evolvono e acquisiscono capacità decisionali. La risposta suggerita dall'approccio comparatistico è volutamente "antieristica": non occorrono nuovi soggetti di diritto né palingenesi concettuali, e non serve nemmeno il ricorso alla fantascienza⁶⁸. Potrebbe occorrere, piuttosto, una complementarità dei rimedi, individuali e collettivi, preventivi e successivi, indisponibili e negoziali, al fine di individuare un punto fermo che nessuna semplificazione possa negoziare. Perché il dato, prima ancora di essere una risorsa del mercato, è una proiezione della persona umana. Ed è la persona, non il mercato né la macchina, a costituire la misura di ogni regola⁶⁹.

⁶⁸ U. PAGALLO, *Data Protection in EU and US Laws and AI: What Legal Changes We Should Expect in the Foreseeable Future?*, cit., pp. 599 ss., il quale osserva che, per riconoscere come l'utilizzo diffuso dell'intelligenza artificiale stia già incidendo sulle basi strutturali delle discipline relative alla privacy e alla protezione dei dati, non è necessario ipotizzare sistemi provvisti di caratteristiche umane o di intelligenze sovrumane: le maggiori criticità, imprevedibilità dei sistemi, opacità, bias, perdita di contesto, discriminazioni e sorveglianza, sono chiaramente verificabili nelle applicazioni attuali e giustificano un approccio regolatorio proattivo.

⁶⁹ S. RODOTÀ, *Il diritto di avere diritti*, cit., dove si sottolinea il concetto della persona quale misura irrinunciabile dell'innovazione giuridica e tecnologica; e G. RESTA, *Dignità, persone, mercati*, cit., dove si dimostra che il mercato degli attributi personali è ammissibile soltanto nei limiti che la logica dignitaria gli assegna: coordinate all'interno delle quali il diritto privato dei dati può accogliere l'intelligenza artificiale senza esserne snaturato.

DIRITTO MERCATO TECNOLOGIA

Numeri Speciali

- | | |
|------|---|
| 2016 | LO STAUTO ETICO GIURIDICO DEI CAMPIONI BIOLOGICI UMANI
a cura di Dario Farace |
| 2017 | IL MERCATO UNICO DIGITALE
a cura di Gianluca Contaldi |
| 2018 | LA RICERCA SU MATERIALI BIOLOGICI DI ORIGINE UMANA:
GIURISTI E SCIENZIATI A CONFRONTO
a cura di Alberto M. Gambino, Carlo Petrini e Giorgio Resta |
| 2019 | LA TASSAZIONE DELL'ECONOMIA DIGITALE TRA SVILUPPI RECENTI
E PROSPETTIVE FUTURE
a cura di Alessio Persiani |

La rivista “Diritto Mercato Tecnologia” intende fornire un costante supporto di aggiornamento agli studiosi e agli operatori professionali nel nuovo scenario socio-economico originato dall’interrelazione tra diritto, mercato e tecnologia, in prospettiva interdisciplinare e comparatistica. A tal fine approfondisce, attraverso studi nei settori privatistici e comparatistici, tematiche afferenti in particolare alla proprietà intellettuale, al diritto antitrust e della concorrenza, alle pratiche commerciali e alla tutela dei consumatori, al biodiritto e alle biotecnologie, al diritto delle comunicazioni elettroniche, ai diritti della persona e alle responsabilità in rete.

