Tecnologie assistive “AI based” e tutela delle persone con disabilità: privacy e responsabilità nel diritto privato europeo, britannico e comparato

5 Marzo 2026

Introduzione

Dalla nascita simbolica dell’intelligenza artificiale alla Conferenza di Dartmouth del 1956, il rapporto tra cognizione e automazione ha posto profonde sfide giuridiche ed etiche (McCarthy et al., 1955). In quella che Schwab (2016) ha definito la “Quarta rivoluzione industriale”, l’IA sta trasformando l’interazione umana con la tecnologia, in particolare nei contesti di vulnerabilità strutturale (NYC, 2025). Tra gli sviluppi più promettenti vi sono le tecnologie assistive basate sull’IA, che migliorano la comunicazione, la percezione e la mobilità delle persone con disabilità. Dagli strumenti attivati dalla voce alle interfacce cervello-computer (BCI), questi sistemi favoriscono autonomia e inclusione. Tuttavia, la loro dipendenza dall’elaborazione di grandi quantità di dati e da algoritmi adattivi genera rilevanti criticità in materia di protezione dei dati, consenso e responsabilità civile (Murray, 2020).

Questo saggio esamina tali questioni alla luce del diritto privato europeo, britannico e comparato. Analizza come il GDPR dell’UE e l’AI Act interagiscano con l’UK GDPR e con il Data Protection Act 2018, nonché il modo in cui i regimi di responsabilità nei sistemi di civil law e common law

affrontano i danni causati dall'IA assistiva. L'obiettivo è valutare se i quadri normativi esistenti proteggano adeguatamente le persone la cui disabilità le rende dipendenti da queste tecnologie.

1. **Protezione dei dati e consenso nei contesti assistivi**

I sistemi di IA assistiva trattano abitualmente categorie particolari di dati, tra cui informazioni biometriche, neurali e comportamentali. Ai sensi dell'articolo 9 del GDPR, tale trattamento è lecito solo in presenza di specifiche eccezioni, la più comune delle quali è il consenso ai sensi dell'articolo 6, paragrafo 1, lettera a). Tuttavia, quando gli utenti non possono esprimere o revocare liberamente il consenso a causa di disabilità cognitive o comunicative, questa base giuridica diventa fragile. Come sostiene Pizzetti (2018), il consenso non può fungere da reale garanzia quando l'autonomia è strutturalmente limitata.

Nei contesti assistivi, il consenso può essere mediato da caregiver o da interfacce tecnologiche, con il rischio di forme di eterodeterminazione e di opacità procedurale (Hervey & Lavy, 2024). Tali rischi aumentano quando il sistema di IA è qualificato come ad alto rischio ai sensi dell'articolo 6 dell'AI Act, che impone obblighi di gestione del rischio e di supervisione umana. Tuttavia, questi obblighi potrebbero non garantire un controllo effettivo da parte dell'utente quando le persone non hanno la capacità di comprendere il funzionamento degli algoritmi o le sue implicazioni per i loro diritti.

L'interazione tra l'AI Act e il GDPR rimane oggetto di dibattito. Il Garante italiano ha osservato che l'AI Act «opera come una normativa aggiuntiva sull'uso e la condivisione dei dati», sovrapponendosi ai principi del GDPR relativi alla limitazione delle finalità e alla

responsabilizzazione (accountability). Analogamente, la Conferenza tedesca delle autorità per la protezione dei dati (DSK, 2024) ha evidenziato l'incertezza che tale sovrapposizione genera per i titolari del trattamento. Al centro della questione vi è la classificazione dei dati: mentre il GDPR distingue tra dati personali e dati non personali (articolo 4, paragrafo 1), questo confine è messo in discussione dalla capacità dell'IA di correlare dataset eterogenei e di re-identificare individui a partire da dati apparentemente anonimi. Le banche dati ibride, che combinano entrambe le tipologie, sono soggette al GDPR quando i dataset sono «inestricabilmente collegati» (Wachter et al., 2017).

Il problema diventa ancora più complesso nel caso delle neurotecnologie, che elaborano dati neurali e mentali in grado di rivelare emozioni, ricordi o intenzioni. D'Acunto e Mollo (2022) osservano che, mentre i dati neurali possono qualificarsi come dati personali, i dati mentali sono più difficili da classificare al di fuori dei contesti clinici. Di conseguenza, alcuni degli aspetti più sensibili della cognizione umana rischiano di rimanere al di fuori della protezione prevista dall'articolo 9 del GDPR, salvo nei casi in cui rivelino caratteristiche come convinzioni politiche o religiose.

II. Il quadro britannico: dall'UK GDPR al Data Protection Act 2018

Dopo la Brexit, il Regno Unito ha mantenuto l'UK GDPR, affiancato dal Data Protection Act 2018 (DPA 2018). Il quadro normativo britannico ricalca in larga misura il modello europeo, ma prevede ulteriori meccanismi volti a garantire un trattamento leale e lecito dei dati e maggiori tutele per le persone vulnerabili. L'Information Commissioner's Office (ICO, 2023) sottolinea in particolare il principio di *fair processing*, che impone ai titolari del trattamento di assicurare che gli individui comprendano come i loro dati vengano utilizzati, soprattutto quando i processi decisionali

coinvolgono sistemi di IA o forme di profilazione automatizzata.

Il sistema britannico riconosce inoltre la difficoltà di ottenere un consenso valido da parte di utenti con capacità limitata. Ai sensi della sezione 9 del DPA 2018, il trattamento di categorie particolari di dati è consentito se ricorre una delle condizioni previste nello *Schedule 1*. Tra queste, lo *Schedule 1, Part 2, Paragraph 6* permette il trattamento per motivi di rilevante interesse pubblico, purché siano previste adeguate garanzie. Le linee guida dell'ICO su IA e protezione dei dati (2023) sottolineano inoltre che il principio di equità implica la possibilità di "contestare in modo significativo" decisioni automatizzate, un aspetto particolarmente rilevante per i sistemi assistivi che mediano la voce o le intenzioni di un utente (ICO, 2023).

Anche la giurisprudenza britannica si è confrontata direttamente con questioni di privacy legate all'IA. Nel caso *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, la Court of Appeal ha stabilito che l'uso del riconoscimento facciale in tempo reale da parte della polizia violava il diritto alla vita privata ai sensi dell'articolo 8 della Convenzione europea dei diritti dell'uomo e mancava di una chiara base giuridica nel DPA 2018. La decisione ha evidenziato la necessità di trasparenza, proporzionalità e controllo, principi che richiamano il quadro di responsabilizzazione (*accountability*) previsto dal GDPR. Tuttavia, come osservato dallo stesso ICO, il diritto britannico attuale non prevede garanzie specifiche per l'IA assistiva che elabora neurodati o flussi continui di dati comportamentali, lasciando gli utenti esposti a possibili abusi o discriminazioni (CJEU, C-621/15, 2017).

III. Responsabilità civile e prospettive comparate

La responsabilità per i danni causati dalle tecnologie assistive basate sull'IA rimane una delle questioni più controverse nei diversi ordinamenti. Nei sistemi di *civil law*, la responsabilità si fonda tradizionalmente sulla colpa o sul difetto del prodotto, ma queste categorie risultano messe alla prova da sistemi auto-apprendenti i cui processi causali sono opachi. Il ritiro, nel 2025, della proposta di AI Liability Directive dell'UE (COM(2022) 496 final) ha lasciato un vuoto normativo. La Product Liability Directive (UE) 2024/2853 colma solo in parte questa lacuna, estendendo la nozione di difetto anche al software e agli output dell'IA. Tuttavia, come osservano Procida Mirabelli Di Lauro e Feola (2020), questo modello resta essenzialmente reattivo e tecnologicamente statico.

La giurisprudenza comparata mostra tentativi di adattare i principi esistenti. La Corte di giustizia dell'Unione europea (CJEU, C-621/15, 2017) ha riconosciuto che i ricorrenti possono fare affidamento su presunzioni di difetto, alleggerendo l'onere probatorio. Anche la Corte di cassazione italiana (Cass. civ., Sez. III, 22571/2018) si è sostanzialmente allineata a questo orientamento, riconoscendo il carattere "presunto" della responsabilità per prodotto difettoso e ammettendo il ricorso a presunzioni probatorie per evitare che il danneggiato sia gravato da un onere della prova impossibile. Analogamente, la Corte federale tedesca (BGH, VI ZR 107/08, 2009) ha riconosciuto una convergenza tra colpa e difetto, rafforzando la finalità protettiva del diritto della responsabilità civile.

Nel *common law* britannico, la responsabilità per i sistemi di IA resta ancorata al paradigma della negligence. In base al caso *Caparo Industries plc v Dickman* [1990] 2 AC 605, la responsabilità richiede la prevedibilità del danno (*foreseeability*), la prossimità (*proximity*) e l'esistenza di un dovere di diligenza (*duty of care*). Questi elementi diventano problematici quando il danno deriva da sistemi

autonomi o auto-apprendenti che evolvono oltre la loro programmazione iniziale. Nel caso *Robinson v Chief Constable of West Yorkshire Police* [2018] UKSC 4, la Supreme Court ha ribadito che i doveri giuridici devono fondarsi su principi consolidati piuttosto che su valutazioni discrezionali di politica del diritto, ma ha lasciato aperta la questione di come tali doveri si applichino ai danni causati da algoritmi. Inoltre, nell'ambito della responsabilità da prodotto disciplinata dal Consumer Protection Act 1987, il software non è esplicitamente elencato tra i "prodotti", creando ulteriore incertezza nel caso di strumenti di IA difettosi.

In prospettiva comparata, modelli di responsabilità basati sul rischio o schemi di assicurazione obbligatoria – come proposto da parte della dottrina europea – potrebbero offrire una soluzione più flessibile (Procida Mirabelli Di Lauro & Feola, 2020). Tali meccanismi garantirebbero il risarcimento degli utenti, in particolare delle persone con disabilità, anche quando colpa o nesso causale non possano essere pienamente dimostrati. Essi sarebbero inoltre coerenti con la logica preventiva sia dell'AI Act sia dei principi britannici di gestione proporzionata del rischio.

IV. Privacy e responsabilità civile: verso un quadro coerente

La regolazione della protezione dei dati e della responsabilità civile presenta una significativa frammentazione tra i diversi sistemi giuridici. Il GDPR e l'AI Act dell'Unione europea pongono l'accento sulla prevenzione e sulla trasparenza, mentre il Data Protection Act 2018 (DPA 2018) del Regno Unito e le linee guida dell'ICO si concentrano maggiormente sull'equità del trattamento e sui rimedi individuali. Tuttavia, nessuno di questi strumenti offre una soluzione completa, né per gli utenti danneggiati da malfunzionamenti o da un uso improprio delle tecnologie assistive basate sull'IA, né per coloro che subiscono violazioni dei dati personali causate da malfunzionamenti o da un uso improprio del sistema di IA.

Per quanto riguarda la responsabilità per le violazioni dei dati personali, l'articolo 82 del GDPR e la sezione 168 del DPA 2018 riconoscono agli interessati il diritto al risarcimento. In pratica, tuttavia, dimostrare il nesso causale e quantificare il danno resta complesso quando il funzionamento del sistema di IA è opaco o mediato da piattaforme di terze parti. I tribunali potrebbero affrontare questa difficoltà interpretando le norme sul risarcimento alla luce dell'articolo 47 della Carta dei diritti fondamentali dell'Unione europea – che sancisce il diritto a un ricorso effettivo – e dell'articolo 6 della Convenzione europea dei diritti dell'uomo – relativo al diritto a un equo processo – assicurando così che le persone vulnerabili non siano private di tutela anche quando il danno presenti una complessità tecnologica.

Per quanto riguarda invece la responsabilità civile generale per i danni derivanti da malfunzionamenti o dal comportamento dei sistemi di IA assistiva, dottrina e giurisprudenza stanno esplorando modelli di imputazione sistemica, riconoscendo il ruolo attivo delle architetture algoritmiche. Sul piano concettuale, la teoria degli "agenti elettronici" elaborata da Teubner mette in discussione le premesse antropocentriche del diritto, suggerendo che le architetture digitali possano agire come soggetti semi-autonomi nella produzione di effetti giuridici. Sebbene i tribunali nelle giurisdizioni di *common law*, come nel caso *Thaler v Commissioner of Patents* [2021] FCA 879, abbiano resistito all'idea di riconoscere personalità giuridica all'IA (Teubner, 2006), Wagner (2019) sostiene che il diritto privato dovrà evolversi in questa direzione.

Conclusione

Le tecnologie assistive basate sull'IA rappresentano al tempo stesso il potenziale emancipatorio e i rischi dell'innovazione digitale. Da un lato, offrono opportunità straordinarie per

rafforzare l’autonomia e l’inclusione delle persone con disabilità; dall’altro, le espongono a nuove forme di vulnerabilità. L’analisi comparata del diritto europeo, britannico e tedesco-italiano mostra progressi significativi nella regolazione della protezione dei dati e della gestione del rischio, ma anche persistenti lacune in materia di responsabilità e rimedi.

Il GDPR, l’AI Act, l’UK GDPR e il DPA 2018 forniscono nel loro insieme una base fondata su equità, responsabilizzazione e trasparenza. Tuttavia, il consenso resta fragile nei contesti di dipendenza, e le dottrine della responsabilità civile – siano esse fondate sulla colpa o sul difetto del prodotto – faticano ad adattarsi a sistemi autonomi. Un quadro normativo più coerente dovrebbe combinare garanzie preventive con meccanismi di risarcimento basati sul rischio, in modo da evitare che l’innovazione tecnologica accentui le disuguaglianze.

In definitiva, la sfida per il diritto privato consiste nel conciliare la vulnerabilità umana con l’autonomia tecnologica, integrando l’IA in un ordine giuridico capace di tutelare la dignità e l’autodeterminazione di ogni individuo, compresi coloro la cui voce è mediata da macchine intelligenti.

Bibliography

Libri e capitoli di libro

- D’Acunto, L. & Mollo, A.A., “Profili di un’analisi etica e giuridica delle neurotecnologie in funzione di tutela delle persone con disabilità”, in Dell’Aversana, F., Fattori, L., Mollo, A.A. & Napolitano, D. (eds.), *Note sulla disabilità* (Naples: Editoriale Scientifica, 2022).
- Hervey, M. & Lavy, M. (eds.), *The Law of Artificial Intelligence* (London: Sweet & Maxwell, 2024).
- Murray, S., *Disability and the Posthuman: Bodies,*

Technology and Cultural Futures (Liverpool: Liverpool University Press, 2020).
- Pizzetti, F. (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione* (Turin: Giappichelli, 2018).
- Procida Mirabelli Di Lauro, A. & Feola, M., "Intelligenze Artificiali e responsabilità civile", in *Diritto delle obbligazioni* (Naples: Edizioni Scientifiche Italiane, 2020), 507–558.
- Schwab, K., *La quarta rivoluzione industriale* (Milan: FrancoAngeli, 2016).

Articoli su rivista

- Teubner, G., "Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law", *Journal of Law and Society*, 33(4), 497–521 (2006).
- Wagner, G., "Robot, Inc.: Personhood for Autonomous Systems?", *Fordham Law Review*, 88, 591–612 (2019).
- Wachter, S., Mittelstadt, B. & Floridi, L., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR", *International Data Privacy Law*, 7(2), 76–99 (2017).

Report

- Garante per la protezione dei dati personali, I*ntelligenza artificiale e protezione dei dati: tra innovazione e tutela dei diritti fondamentali* (2023).
- German Data Protection Conference (DSK), *Orientation Guide on AI and Data Protection* (2024).
- Information Commissioner's Office, *AI and Data Protection Guidance* (London, 2023).
- McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E., *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence* (Dartmouth, 1955).
- New York City Bar Association, *The Impact of the Use of AI on People with Disabilities* (2025).

Giurisprudenza

- BGH, VI ZR 107/08 (2009).
- Caparo Industries plc v Dickman [1990] 2 AC 605.
- civ., Sez. III, n. 22571 (2018).
- CJEU, C-621/15 (2017).
- R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058.
- Robinson v Chief Constable of West Yorkshire Police [2018] UKSC 4.
- Thaler v Commissioner of Patents [2021] FCA 879.