Digeat N.9 - 19 Marzo 2026

L’identità vulnerabile: etica e diritto nell’era della re-identificazione permanente

Di Paolo Assirelli

Abstract

Il superamento del concetto di Stato-nazione, messo in crisi dall’azione globale delle big tech, sta erodendo la sovranità individuale e statale sul controllo informativo. La stessa natura e l’implementazione dei dataset longitudinali – insiemi di dati raccolti osservando le stesse unità analitiche attraverso più punti temporali successivi – rende sempre più illusoria l’anonimizzazione perfetta, in qualche modo preconizzata dalla dicotomia tra dato anonimo e pseudonimizzato già presente nel GDPR . Ne consegue una vulnerabilità strutturale dell’identità personale, ontologicamente fragile di fronte alla granularità temporale, alla *data triangulation* e alla crescente potenza computazionale degli algoritmi predittivi. L’articolo tenta una riflessione su come questa dinamica configuri una crisi sistemica dei diritti fondamentali, con il capitalismo di sorveglianza che trasforma l’esperienza umana in un surplus comportamentale commerciabile, sottraendo alla persona il governo della propria storia biografica. Al di là dell’illusione dell’anonimizzazione irreversibile si sta delineando la necessità di un nuovo paradigma etico-giuridico: una governance risk-based multilivello che, integrando pseudonimizzazione robusta, DPIA dinamiche, data access committees e audit etici permanenti, riesca a custodire l’identità vulnerabile non attraverso l’illusione della sparizione, ma mediante trasparenza, accountability e responsabilità condivisa. In tale prospettiva, il superamento dello Stato-nazione impone una riconfigurazione antropocentrica del diritto digitale, dove avvocati, DPO e ordini professionali sono chiamati ad assumere il ruolo di custodi etici contro l’espropriazione identitaria perpetrata dai nuovi centri di potere algoritmico.

Indice

La fine dell’anonimato come categoria giuridica

Il quadro normativo realizzato dal GDPR riposa su una distinzione che l’evoluzione tecnologica sta rendendo sempre più precaria.

L’art. 4, par. 1, n. 5 qualifica il dato anonimo come informazione riguardante persone fisiche “non identificabili” con i mezzi ragionevolmente disponibili al momento del trattamento. Il Considerando 26 aggiunge un elemento cruciale: tali “mezzi tecnici” includono *“sia la tecnologia attuale sia la tecnologia prevedibile nei prossimi anni”*.

> Appare evidente l’implicito riconoscimento della natura contingente dell’anonimizzazione e l’ancoramento della sua tutela a uno standard dinamico non completamente governato dalla struttura binaria del Regolamento.

D’altro canto, la pseudonimizzazione è definita dall’art. 4, par. 1, n. 6 come misura di sicurezza (art. 32), non di anonimizzazione: **il dato pseudonimizzato rimane pienamente personale**. Le Linee guida EDPB 4/2019 lo ribadiscono con precisione, specificando che non costituisce anonimizzazione alcun trattamento dal quale sia possibile re-identificare l’interessato attraverso informazioni aggiuntive. Il Garante Privacy italiano, nel Provvedimento del 13 novembre 2024, ha confermato questa distinzione in contesti sanitari, sottolineando che la semplice sostituzione di identificativi diretti non garantisce l’uscita dal perimetro GDPR in presenza di variabili indirette.

Le evidenze empiriche smentiscono con forza la mitologia dell’anonimizzazione irreversibile. Il Fascicolo Sanitario Elettronico 2.0, che raccoglie dati clinici longitudinali su milioni di assistiti italiani, è vulnerabile anche con pseudonimizzazione crittografica: sequenze temporali di diagnosi rare, pattern di accesso e correlazioni tra variabili generano impronte uniche, esposte a linkage attacks con fonti esterne.

Le biobanche genomiche presentano un profilo di rischio ancor più radicale: già nel 2018 alcuni studi (Erlich et al.) avevano dimostrato che, incrociando i milioni di profili genomici da database consumer con i dati genealogici pubblici, circa il 60% degli individui di discendenza europea risultava re-identificabile anche senza essere direttamente nel database, riuscendo a coprire l’intera rete dei consanguinei. Sul fronte dei dati di mobilità, già dal 2013, siamo a conoscenza che sono sufficienti quattro punti spazio-temporali per identificare il 95% degli utenti con accuratezza superiore al 90%.

«**Le tecniche standard rivelano limiti strutturali**: la k-anonymity *(tecnica di anonimizzazione che rende ogni record indistinguibile da almeno altri k?1 soggetti, dato un insieme di attributi quasi?identificativi)* risulta vulnerabile a particolari tipologie di attacchi, la differential privacy *(tecnica che aggiunge rumore statistico ai dati o ai risultati per impedire la re?identificazione di singoli individui pur mantenendo l’utilità complessiva del dataset)* può accumulare rumore esponenziale nei dataset longitudinali estesi, ma al prezzo di diminuirne fortemente l’utilità scientifica.» Il *no free lunch theorem* (Wolpert e Macready, 1997) afferma che **non esiste un algoritmo universale ottimale: ogni tecnica eccelle in contesti specifici, fallendo altrove**. Non a caso la ISO/IEC 20889:2018 stabilisce che l’anonimizzazione richiede una valutazione del rischio caso-specifica e non una garanzia assoluta.

> La conclusione è ineludibile: l’anonimizzazione è misura probabilistica, non definitiva, e richiede una governance continua che vada ben oltre la sola dimensione tecnica.

L’identità come bene relazionale e vulnerabile

Nel tradizionale lessico giuridico l’identità personale è trattata come un insieme statico di attributi, funzionale all’imputazione di situazioni giuridiche soggettive. Questa impostazione rivela la propria insufficienza non appena il dato cessa di essere mera etichetta identificativa per diventare strumento di modellazione dei comportamenti in un ecosistema digitale pervasivo.

Paul Ricœur ha mostrato che l’identità non è una sostanza immobile ma il risultato sempre provvisorio del racconto che la persona costruisce su se stessa, integrando memoria, eventi, relazioni e proiezioni

future: la narrazione media tra idem (ciò che resta) e ipse (ciò che cambia).

> **I dati personali non sono quindi semplici “pezzi di informazione”, ma sedimenti della storia narrativa dell’individuo.**

Nei dataset longitudinali questa dimensione emerge con forza: il fascicolo sanitario, le tracce di mobilità, le interazioni online non descrivono solo uno stato, ma configurano una traiettoria biografica che può essere letta, interpretata e categorizzata da terzi senza il controllo del soggetto interessato.

> Sul piano dei diritti fondamentali, l’art. 8 CEDU è stato progressivamente interpretato dalla Corte europea dei diritti dell’uomo come comprensivo del diritto all’identità personale e allo sviluppo della propria personalità.

In decisioni recenti, come Mitrevska c. Macedonia del Nord, la Corte ha ribadito che l’art. 8 impone allo Stato anche obblighi positivi di predisporre procedure effettive di accesso a informazioni essenziali per la costruzione della propria identità, incluse informazioni sanitarie sui genitori biologici. I dati genetici rappresentano il caso limite: strutturalmente relazionali perché riguardano anche i consanguinei, di fatto non anonimizzabili in modo assoluto senza distruggere la loro utilità scientifica.

> **La vulnerabilità identitaria si colloca a un duplice livello: da un lato il rischio di re-identificazione non autorizzata**, con violazione della riservatezza e della dignità; **dall’altro il rischio di espropriazione narrativa**, quando le informazioni su origini, salute e comportamenti sono gestite e rese opache, impedendo all’individuo di accedere alla propria storia o di contestare la narrazione che altri costruiscono su di lui. L’identità diventa vulnerabile alla super-esposizione – quando l’accumulo di correlazioni rende la persona radicalmente trasparente a soggetti terzi – e alla distorsione, quando le rappresentazioni algoritmiche consolidano stereotipi e discriminazioni che la persona non può correggere.

Il capitalismo di sorveglianza come espropriazione sistemica

Nel paradigma del capitalismo di sorveglianza, descritto da Shoshana Zuboff, l’esperienza umana viene sistematicamente trasformata in surplus comportamentale incorporato in modelli predittivi che determinano cosa vediamo, quali offerte riceviamo, quali opportunità ci vengono concesse o negate. Ogni interazione digitale – click, posizione GPS, ricerca, tempo di permanenza su una pagina – viene registrata, categorizzata e tradotta in merce venduta a inserzionisti, società private e governi per modulare il comportamento individuale.

Nei dataset longitudinali il processo acquisisce una dimensione temporale qualitativamente nuova: non più mere istantanee statiche, ma traiettorie comportamentali complete che permettono di anticipare chi saremo domani. In ambito creditizio e assicurativo, algoritmi come quelli di Upstart o Lemonade costruiscono profili di rischio da pattern di mobilità e acquisti, determinando l’accesso al credito indipendentemente dalla solvibilità oggettiva. Le piattaforme come YouTube e TikTok usano dati longitudinali per ottimizzare raccomandazioni non in funzione della verità, ma del tempo di permanenza, rinchiudendo gli utenti in camere d’eco che consolidano polarizzazioni cognitive.

> Tutto ciò configura una vera espropriazione sistemica: l’esperienza personale, che dovrebbe essere dominio della sovranità individuale, viene convertita in proprietà privata di corporation che ne detengono l’uso commerciale esclusivo.

Google, Meta, Amazon e TikTok esercitano un potere extraterritoriale con algoritmi proprietari non accessibili agli Stati. Il GDPR e l'AI Act hanno portata extraterritoriale solo in virtù del mercato UE (Brussels Effect), ma non possono imporre accesso ai codici sorgente né ai dataset di training. Il risultato è una privatizzazione della sovranità che erode sia il controllo statale sia l'autodeterminazione individuale, rendendo urgente l'elaborazione di una data sovereignty personale comprensiva di diritti di portabilità narrativa, contestazione algoritmica e compartecipazione ai benefici del surplus comportamentale.

Prospettive normative e governance multilivello

Appare chiaro che **il GDPR**, pur rimanendo la chiave di volta della protezione dei dati in Europa, **non può riuscire** – mercé la sua logica orizzontale e binaria – a governare la complessità dei dataset longitudinali.

> Di qui il moltiplicarsi di **regolazioni settoriali (Data Governance Act, Data Act, AI Act e soprattutto European Health Data Space (EHDS))** che stanno disegnando una **nuova fase dell'approccio risk-based**: non più centrato sulla promessa di far "sparire" i dati dal campo del diritto tramite anonimizzazione, ma **sulla costruzione di un regime di condivisione condizionata e vigilata**.

L'EHDS, adottato come Regolamento nel 2025, **istituisce uno spazio europeo comune dei dati sanitari su tre assi**: **rafforzamento del controllo** dei cittadini, **creazione di un mercato unico** per i servizi di sanità digitale, **definizione di regole per il riuso di dati** per finalità di interesse pubblico. Ogni Stato membro deve istituire almeno una Health Data Access Body (HDAB – autorità nazionale incaricata, nell'EHDS, di valutare le richieste di accesso e autorizzare il riuso dei dati sanitari per finalità secondarie, garantendo sicurezza, etica e tutela dei diritti) per valutare le richieste di accesso, rilasciare *data permits* e vigilare sulle secure processing environments.

> In tale disegno, l'anonimizzazione cessa di essere condizione statica per diventare requisito tecnico coniugato con misure organizzative e procedurali da rivedere periodicamente.

L'AI Act (Reg. UE 2024/1689) **classifica i sistemi di IA per livelli di rischio e sottopone quelli "ad alto rischio"** – comprese applicazioni sanitarie, creditizie e di accesso a servizi essenziali – **a obblighi stringenti di trasparenza, documentazione e conformità ex ante**. «L'art. 27 impone, per alcune categorie, una valutazione d'impatto sui diritti fondamentali (FRIA *(Fundamental Rights Impact Assessment, analisi preventiva degli impatti dei sistemi di IA ad alto rischio sui diritti fondamentali ai sensi dell'art. 27 AI Act)*) distinta dalla DPIA privacy, con analisi degli impatti su gruppi vulnerabili e meccanismi di reclamo. Il legislatore riconosce così esplicitamente che l'uso di dati longitudinali da parte dell'IA incide sulla non discriminazione, sull'accesso ai servizi, sulla dignità e sull'autonomia.

«Sul piano tecnico, il federated learning *(metodo di addestramento di modelli di IA in cui i dati restano localmente nei singoli enti e si condividono solo parametri o aggiornamenti del modello, riducendo i trasferimenti di dati grezzi)*, le tecniche di privacy-preserving record linkage *(insieme di tecniche che consentono di collegare record riferiti alla stessa persona presenti in banche dati diverse minimizzando la rivelazione di dati identificativi)* e gli ambienti sicuri di trattamento costituiscono pilastri complementari di questa governance, nessuno dei quali è di per sé sufficiente in contesti ad alta dimensionalità e longitudinalità.»

La **Legge italiana 132/2025 sull'IA aggiunge** un ulteriore tassello **per le professioni intellettuali**: l'utilizzo di sistemi algoritmici è **ammesso solo per attività strumentali e di supporto**, con

prevalenza del lavoro umano **e obbligo di informativa chiara e preventiva al cliente**.

L’Etica della responsabilità nell’epoca dell’incertezza

L’enciclica *Laudato si’* con la formula «tutto è connesso», ha indicato che crisi ambientale e crisi sociale sono manifestazioni di un’unica crisi socio-ambientale, applicandola al mondo dei dati, diviene una chiave interpretativa che consente di riconoscere come i dataset longitudinali non siano strumenti neutri, ma ambienti di vita in cui si gioca la distribuzione del potere e la stessa possibilità di custodire l’identità personale. Il paradigma tecnocratico criticato da Papa Francesco – che riduce il reale a materia disponibile per un’élite tecnico-economica – trova nel capitalismo di sorveglianza la sua declinazione più compiuta: **l’estrazione incontrollata di dati personali non è meno lesiva della dignità umana dell’estrazione di risorse naturali**.

> Una vera conversione ecologica richiede pertanto anche una conversione digitale, in cui i criteri di giustizia, solidarietà e cura dei più fragili orientino la progettazione delle piattaforme, l’uso dei dati e la distribuzione dei benefici dell’innovazione. **In questo contesto, il ruolo dell’avvocatura assume una rilevanza nuova**.

La Legge 132/2025 sull’IA ha formalizzato principi già presenti nel dibattito deontologico: l’avvocato ha l’obbligo di informare il cliente sull’impiego di sistemi algoritmici nella prestazione professionale ed ai quali non può – in nessun caso – delegare il nucleo essenziale della propria opera intellettuale. Ma il mandato dell’avvocato come custode dell’identità vulnerabile va oltre la conformità formale: egli può contestare narrative algoritmiche ingiuste in giudizio, far emergere i profili discriminatori di modelli di scoring in sede regolatoria, negoziare clausole contrattuali che limitino la profilazione e il riuso non controllato dei dati.

> Ciò implica una deontologia arricchita: comprensibilità tecnologica, trasparenza verso il cliente sui rischi legati ai dati longitudinali, vigilanza sull’equità dei processi decisionali automatizzati che incidono su diritti e libertà.

Il **dibattito internazionale** intorno ai concetti di **data dignity e data as labor** (proposti da Lanier e Glen Weyl) suggerisce di **considerare i dati come esito di un’attività che merita riconoscimento e controllo**, non solo come oggetto di protezione. Da un punto di vista giuridico-fondamentale, questa istanza sembra richiedere **il riconoscimento di un diritto alla storia personale in tre dimensioni**: **il diritto ad accedere alla propria biografia digitale in forma comprensibile**, superando le opacità delle black box; **il diritto a contestare narrazioni algoritmiche scorrette o discriminatorie**, chiedendo la rettifica *delle inferenze e non solo dei dati fattuali*; **il diritto a partecipare alle decisioni collettive sul riuso dei dati per finalità di ricerca e governance pubblica**. Questo diritto si pone in continuità con l’evoluzione dell’art. 8 CEDU e dell’art. 8 Carta UE, declinandoli in forma più aderente all’ecosistema digitale contemporaneo.

Conclusioni

> In questa prospettiva, la conversione digitale non resta un compito astratto del legislatore o delle piattaforme, ma ridisegna anche la deontologia forense, chiamando l’avvocato a farsi custode operativo dell’identità vulnerabile nei contesti decisionali governati da dati e algoritmi.

L’identità vulnerabile non è quindi un mero incidente di percorso, ma assurge ormai a cifra strutturale della condizione umana nell’ecosistema dei dati longitudinali.

La promessa normativa dell'anonimizzazione irreversibile si sta progressivamente rivelando una costruzione teorica incapace di reggere all'urto combinato di granularità temporale, interoperabilità sistemica e potenza computazionale. L'identità personale – intesa come trama narrativa e relazionale, non come fascio statico di attributi – viene allo stesso tempo progressivamente esposta a re-identificazione permanente, profilazione anticipante e manipolazione sottile, con erosione simultanea del diritto alla riservatezza e del diritto all'autodeterminazione.

I sistemi regolatori più recenti confermano la necessità di questo cambio di paradigma. L'EHDS affida agli Health Data Access Bodies e ai comitati etici il bilanciamento tra interessi pubblici e diritti individuali in una logica di responsabilità condivisa. L'AI Act riconosce che l'uso di dati longitudinali da parte dell'IA incide su uguaglianza, non discriminazione, accesso ai servizi e partecipazione democratica, richiedendo un controllo ex ante. Studi recenti mostrano tuttavia come anche i framework più avanzati, inclusi quelli promossi dal NIST, fatichino a misurarsi adeguatamente con i rischi di inferenza e linkage tipici dei grandi dataset: la privacy di questi sistemi deve essere trattata come gestione del rischio, non come garanzia assoluta.

La categoria di identità vulnerabile – davanti al potere di fatto esercitato dalle grandi piattaforme sulla vita informativa delle persone travalicando le giurisdizioni tradizionali – sembra in grado offrire la possibilità di compiere un salto concettuale decisivo: **vulnerabile non è solo il soggetto debole, ma chiunque possa essere esposto all'uso dei propri dati in modi che sfuggono al suo controllo**.

Il passaggio da una tutela puramente difensiva (diritto all'oblio, cancellazione) a una tutela proattiva della storia personale – intesa come diritto a governare, comprendere e contestare le narrazioni algoritmiche che ci riguardano – può costituire uno dei terreni più fecondi per ripensare, *"oltre gli Stati"*, il nesso tra sovranità, diritti e centri di potere nell'età globale.

Bibliografia

- Regolamento (UE) 2016/679 – Regolamento generale sulla protezione dei dati – GDPR.
- Regolamento (UE) 2024/1689 – AI Act.
- Regolamento (UE) 2025/327 – European Health Data Space – EHDS.
- Regolamento (UE) 2022/868 – Data Governance Act – DGA.
- Article 29 Data Protection Working Party (WP29), Opinion 4/2007 on the concept of personal data (WP136), adottata il 20 giugno 2007, Bruxelles, 2007 e Working document on Genetic Data (WP91), adottato il 17 marzo 2004, Bruxelles, 2004.
- European Data Protection Board (EDPB), Guidelines 4/2019 on Article 25, Bruxelles, 20 ottobre 2020.
- Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), Roma 4 novembre 1950.
- Carta dei diritti fondamentali dell'Unione europea, 7-12 dicembre 2007.
- Legge 9 agosto 2025, n. 132, Disposizioni in materia di intelligenza artificiale.
- Garante Privacy, Provvedimento 13 novembre 2024 – Misure di pseudonimizzazione nei trattamenti sanitari, doc. web n. 10095724, Roma, 2024.
- Ricœur P., Sé come un altro, Jaca Book, Milano, 2011.
- Zuboff S., Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri, Luiss University Press, Roma, 2019.
- Erlich Y., Shor T., Pe'er I., Carmi S., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, in Science, vol. 362, n. 6415, 9 novembre 2018, pp. 690–694. DOI: 10.1126/science.aau4832.
- Lanier J., Weyl E.G., *A Blueprint for a Better Digital Society*, in Harvard Business Review, 26 settembre 2018 (disponibile all'indirizzo: https://hbr.org).
- Wolpert D.H., Macready W.G., *No Free Lunch Theorems for Optimization*, in IEEE Transactions on Evolutionary Computation, vol. 1, n. 1, aprile 1997, pp. 67–82. DOI: 10.1109/4235.585893.
- Papa Francesco, Lettera enciclica Laudato si': sulla cura della casa comune, Libreria Editrice Vaticana, Città del Vaticano, 24 maggio 2015.