CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

L´ORIZZONTE DEL SIMULACRO E LA MAGNIFICA HUMANITAS. L´AVATAR COME STRUMENTO DI DECEZIONE. L´IMPATTO DELL´IA ACT E DELL´ART. 2-TERDECIES DEL CODICE PRIVACY

L'evoluzione dell'Intelligenza Artificiale (IA), ha trasposto il concetto di immortalità dal dominio della metafisica a quello dell'ingegneria del software. Attraverso la creazione di avatar interattivi, digital twin, e "deadbots", le aziende del settore della Digital Afterlife promettono di preservare non solo la memoria, ma la personalità attiva del defunto. Il presente contributo analizza l'evoluzione di tali sistemi, partendo dall'effetto "ELIZA" del primo chat bot , sino alla costante necessità dell'antropomorfizzazione anche nell'IA.Le moderne tecnologie di telepresenza e i codec avatar a confronto. Esame del quadro normativo vigente, con particolare attenzione al GDPR, all'IA Act e all'innovativo Articolo 2-terdecies del Codice Privacy italiano e la sfida del Magistero del Papa.

di **Annamaria De Gaetano**
IUS/01 - DIRITTO PRIVATO
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Alessio Giaquinto

CamminoDiritto.it
ISSN 2421-7123

Pubblicato, Venerdì 5 Giugno 2026

CamminoDiritto.it
ISSN 2421-7123

Abstract ENG

The evolution of Artificial Intelligence (AI) has transposed the concept of immortality from the realm of metaphysics to that of software engineering. Through the creation of interactive avatars, digital twins, and ”deadbots,” companies in the Digital Afterlife sector promise to preserve not only the memory, but the active personality of the deceased.This paper analyzes the evolution of these systems, from the ”ELIZA” effect of the first rudimentary chatbot to the constant human need for anthropomorphization, even in AI. Modern telepresence technologies and avatar codecs are compared. The current regulatory framework is examined, with particular attention to the GDPR,the AI Act, and the innovative Article 2-terdecies of the Italian Privacy Code and the challenge of the Pope´s Magisterium

---

Sommario: 1. Introduzione: la dimensione giuridica dell’immortalità digitale. 2. Evoluzione storica e tecnologica: dal right to be let alone all'effetto ELIZA. 3. Antropomorfismo: Codec Avatar e Telepresenza. 4. Criticità: sistemi con riconoscimento facciale (SPID) e presenza fisica reale. 5. L'industria dei Dead Bots: attori del mercato e modelli di business. 6. Normativa e qualificazione giuridica in Italia e nel mondo. 7. Il Quadro Europeo: GDPR e IA Act. 8. Situazione italiana. 9. Ermeneutica Costituzionale: l’identità digitale come diritto inviolabile, e Articolo 2-terdecies del Codice Privacy. 10. Articolo 2-terdecies del Codice Privacy 11. Profili penali e sanzioni: la Legge 132/2025 e precedenti storici. 12. Il vuoto normativo e il "consenso per impostazione predefinita". 13. L’eredità digitale. 14. La violazione dell'integrità della persona postuma. 15. La necessità di "Genuine Presence Assurance". 16. Verso nuovi diritti fondamentali: disclosure, spiegazione e controllo umano.17. "Magnifica Humanitas": l'intelligenza artificiale nel solco della Dottrina Sociale. 18. Riflessioni conclusive. 19. Note e riferimenti bibliografici.

1. La dimensione giuridica dell’immortalità digitale

L’immortalità digitale non rappresenta solo una frontiera tecnologica, ma una sfida radicale alla categoria dei diritti della personalità. Sotto il profilo giuridico, essa impone di indagare se la protezione dell'identità possa sopravvivere alla fine biologica del soggetto, trasformando la memoria da deposito statico in un'entità dinamica e interattiva. La "resurrezione digitale" sollecita il giurista a interrogarsi sulla natura del "soggetto digitale" che si affianca a quello fisico, richiedendo una rilettura del sistema dei poteri e delle libertà nella cornice del nuovo costituzionalismo digitale. L’immortalità digitale (o "immortalità virtuale") è il concetto ipotetico di archiviare o clonare la mente e la personalità di un individuo in un substrato digitale, come computer, robot o il

CamminoDiritto.it
ISSN 2421-7123

cyberspazio. Il risultato è un avatar capace di comportarsi, reagire e pensare sulla base dell'archivio digitale della persona originale. Questa "resurrezione digitale" trasforma la memoria da deposito statico (foto, video) in un'entità interattiva, dinamica e conversazionale.

2. Evoluzione storica e tecnologica: dal right to be let alone all'effetto ELIZA

L'analisi storica rivela che la tutela della riservatezza nasce come "diritto di essere lasciato solo" (Warren e Brandeis, 1890), mutuando lo schema proprietario dello ius excludendi alios. Tuttavia, l'evoluzione tecnologica ha spostato il baricentro dalla mera esclusione al controllo proattivo sui dati personali come estrinsecazione della personalità. L'effetto “ELIZA” e l'antropomorfizzazione delle macchine dimostrano la suscettibilità umana nel leggere intenzionalità in semplici software. Tale dinamica, se applicata ai cosiddetti griefbots (o deadbots), crea una "confusione ontologica" che può sfociare in una mercificazione del lutto e in una dipendenza algoritmica, ostacolando il processo psicologico di elaborazione della perdita.I primi tentativi di interazione uomo-macchina risalgono agli anni '60. Nel 1966, Joseph Weizenbaum sviluppò ELIZA, un chatbot che simulava uno psicoterapeuta rogeriano. Il sistema era rudimentale: utilizzava uno script chiamato "DOCTOR" per riformulare le affermazioni degli utenti in domande. Nonostante ELIZA fosse priva di reale comprensione semantica, Weizenbaum fu turbato nello scoprire che esposizioni brevissime potevano indurre pensieri delusionali in persone normali, che iniziavano a confidare segreti profondi alla macchina, convinte di essere comprese. L’effetto “ELIZA” descrive la suscettibilità umana a leggere una comprensione profonda in stringhe di simboli prodotte da computer. È il risultato di una dissonanza cognitiva tra la consapevolezza razionale che il programma è un software e il comportamento emotivo verso di esso. Oggi, questo effetto è amplificato dai moderni modelli linguistici (LLM) che, grazie alla fluidità del linguaggio naturale, rendono la distinzione tra simulazione e realtà quasi impercettibile. Oggigiorno, assistiamo sempre di più al ricorso, da parte di molti adolescenti e non, di umanizzare il rapporto, sino a ricercare consigli ad esempio a Chat GPT: scelte personalissime, vengono affidate all’IA, ignorando la diffusione di dati personalissimi, al solo cliccare del like alla risposta al prompt richiesto.

3. Antropomorfismo: Codec Avatar e Telepresenza - Definizione e Funzionamento

L'antropomorfismo è una tendenza cognitiva universale che porta l'uomo ad attribuire caratteristiche, emozioni e intenzioni umane a entità non umane. Storicamente radicato negli istinti sociali, questo meccanismo aiuta l'uomo a interpretare fenomeni sconosciuti attraverso modelli familiari. Con l'avvento della tecnologia, questa tendenza si è trasferita sugli oggetti intelligenti: l'uso di occhi su un robot o di una voce espressiva in un

CamminoDiritto.it
ISSN 2421-7123

assistente virtuale induce l'utente ad attribuire una coscienza al software. Il pallone da pallavolo " Wilson" con disegnati occhi e capelli dal naufrago Tom Hanks, nel famoso film " Cast Away," è un tipico esempio di come l'uomo ricerca connessioni umane, soprattutto quando si trova in solitudine, o in situazioni in cui è vulnerabile. Le nuove frontiere della simulazione superano il testo per abbracciare il fotorealismo volumetrico. I Codec Avatar di Meta mirano a generare una "presenza sociale" subconscia, simulando segnali non verbali sottili come il movimento degli occhi e i riflessi della luce sulla pelle. Nello specifico, gli intenti sono:

Obiettivo: generare una sensazione subconscia di trovarsi fisicamente con un'altra persona, nonostante la distanza geografica. Meccanismo tecnico: il sistema utilizza sensori di tracciamento oculare e facciale integrati nei visori VR. Questi sensori permettono all'avatar di replicare segnali non verbali estremamente sottili, come il sollevamento di un sopracciglio, lo strizzare degli occhi e persino i riflessi della luce sulla pelle e sulle cornee. Evoluzione della scansione: se inizialmente erano necessarie infrastrutture massive con oltre 100 telecamere, nuove tecniche come il "Gaussian Splatting", permettono oggi, di generare avatar fotorealistici partendo da una semplice scansione effettuata con uno smartphone, democratizzando l'accesso alla creazione di gemelli digitali, ricostruendo fedelmente l'individuo scannerizzato. Attraverso tecniche come il Gaussian Splatting, è oggi possibile creare avatar foto-realistici partendo da una semplice scansione con smartphone, democratizzando l'accesso alla creazione di gemelli digitali tridimensionali per la telepresenza.

4. Criticità: sistemi con riconoscimento facciale (SPID) e presenza fisica reale

L'uso dello SPID (Sistema Pubblico di Identità Digitale) con riconoscimento facciale da remoto, introduce sfide significative nel contesto della diffusione di avatar sempre più realistici, e di tecnologie di manipolazione video. Lo SPID, è definito come la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi. Quando questo riconoscimento avviene "da casa", il sistema deve essere in grado di distinguere tra la presenza fisica reale e una simulazione digitale.

Le principali ripercussioni e rischi legati all'interazione tra questi sistemi di identità e gli avatar includono:

Rischio di Ghost Fraud e Deepfake I criminali informatici, possono utilizzare l'immagine e la voce di una persona (viva o defunta), per creare un avatar capace di superare i sistemi di verifica biometrica. Questo fenomeno, noto come ghost fraud, mira a ottenere accessi non autorizzati a servizi online, conti correnti o benefici previdenziali.

CamminoDiritto.it
ISSN 2421-7123

Vulnerabilità del Riconoscimento Facciale da Remoto Molti sistemi di riconoscimento facciale "da casa" possono essere ingannati da media sintetici o maschere digitali se non dotati di controlli avanzati. Poiché, lo SPID è lo strumento principale per l'identificazione verso la Pubblica Amministrazione e le imprese aderenti, un'usurpazione dell'identità tramite un avatar permetterebbe di compiere atti legali, firmare documenti o accedere a dati sensibili a nome della vittima.

Discrasia tra Identità Reale e Digitale Mentre lo SPID cerca di creare un'identità digitale univoca a fini pubblicistici, la Rete favorisce una "fisiologica multipersonalità", attraverso l'uso di diversi avatar e profili. La sfida giuridica e tecnica è garantire che il "corpo elettronico" (lo SPID) rimanga saldamente ancorato al corpo fisico, evitando che il simulacro (l'avatar) possa operare autonomamente nello spazio legale e amministrativo.

5. L'industria dei Dead Bots: attori del mercato e modelli di business

La "confusione ontologica" causata dai griefbots (o deadbots) consiste nel progressivo sfumare dei confini tra la memoria autentica del defunto e la sua simulazione algoritmica. Questa condizione si verifica quando l'utente non riesce più a distinguere chiaramente tra la realtà dell'assenza biologica e l'illusione della persistenza digitale.

Diverse aziende dominano il mercato della "Digital Afterlife":

DeepBrain AI (Re;memory): crea cloni virtuali che permettono videochiamate con il defunto. HereAfter AI: offre chatbot basati su storie e registrazioni vocali reali. Project December: permette di simulare personalità specifiche pagando un costo contenuto. MyHeritage (Deep Nostalgia): anima foto storiche di antenati tramite IA. **6. Normativa e qualificazione giuridica in Italia e nel mondo.**

Il panorama legislativo mondiale è frammentato: le fonti evidenziano che l'attuale normativa mondiale è spesso repressiva (interviene dopo il danno), piuttosto che proattiva. Manca una distinzione chiara tra l'uso affettivo dei dati dei defunti (griefbots privati) e lo sfruttamento commerciale. Inoltre, le policy contrattuali delle piattaforme Big Tech spesso prevalgono sui diritti degli eredi, creando la necessità di un'uniformazione delle prassi operative a livello globale. Situazione globale:

Europa (GDPR): Il Considerando 27 specifica che il regolamento non si applica ai dati dei defunti, delegando agli stati membri. L'IA Act (dal 2025/2026) imporrà obblighi di trasparenza per i deepfake. Italia: L'Articolo 2-terdecies del Codice Privacy permette l'esercizio dei diritti sui dati del defunto da parte di chi ha un interesse meritevole o

CamminoDiritto.it
ISSN 2421-7123

ragioni familiari. USA: Stati come California e New York riconoscono diritti post-mortem all'immagine e alla voce (NIL rights) per periodi dai 40 ai 70 anni. **7. Il Quadro Europeo: GDPR e IA Act**

La normativa vigente in Europa:

GDPR (Regolamento UE 2016/679): Il regolamento specifica al Considerando 27 che le sue norme sulla protezione dei dati non si applicano alle persone decedute. Esso delega ai singoli Stati membri la facoltà di prevedere norme specifiche per il trattamento dei dati dei defunti IA Act (Regolamento UE 2024/1689): Introduce requisiti rigorosi di trasparenza per i sistemi di IA generativa. Dal 2026, i fornitori di avatar e deepfake dovranno etichettare chiaramente i contenuti, informando gli utenti che stanno interagendo con una simulazione. Alcune pratiche, come la manipolazione subliminale o lo sfruttamento di vulnerabilità (come lo stato di lutto), sono classificate come rischi inaccettabili e vietate dal febbraio 2025. Il Regolamento UE 2024/1689 (IA Act) adotta un approccio basato sul rischio, con finalità chiaramente protettive della dignità umana (criterio teleologico). Dal febbraio 2025, sono vietate le pratiche di manipolazione subliminale che sfruttano le vulnerabilità dei soggetti, incluso lo stato di lutto. Sul piano della trasparenza, i sistemi che generano deepfake o avatar dovranno essere etichettati in modo chiaro, garantendo che l'utente sia consapevole di interagire con una simulazione. Questo dovere di disclosure si configura come il presupposto per l'esercizio di un'autentica autodeterminazione cognitiva. La vigilanza è affidata a un sistema di coordinamento tra l'Ufficio europeo per l'IA e le autorità nazionali, come il Garante Privacy, che dispongono di poteri sanzionatori e strumenti di segnalazione per i cittadini in caso di violazioni o malfunzionamenti. Il Regolamento UE 2024/1689 (IA Act), interviene per prevenire situazioni di "pressione psicologica" che possono portare a gesti estremi. Sono classificate come rischio inaccettabile e vietate (dal febbraio 2025) le pratiche di manipolazione subliminale e lo sfruttamento delle vulnerabilità dei soggetti, incluso lo stato di lutto o la fragilità psicologica **8. Situazione italiana.**

In Italia opera principalmente all'interno del quadro normativo europeo dell'IA Act, integrato da specifiche disposizioni nazionali riguardanti la privacy, i dati dei defunti e le tecnologie di registro distribuito. I pilastri fondamentali della normativa applicabile in Italia in materia di IA sono: i principi costituzionali (art. 2 e 3 Costituzione); IA Act, l'articolo 2-terdecies del Codice Privacy italiano, la Legge 132/2025.

L'Italia, come Stato membro dell'UE, è soggetta all'IA Act, il primo quadro giuridico completo al mondo sull'IA.

Approccio basato sul rischio: la legge classifica i sistemi di IA in quattro livelli

CamminoDiritto.it
ISSN 2421-7123

(Inaccettabile, Alto, Trasparenza, Minimo). Pratiche vietate: dal febbraio 2025, sono vietate in Italia (e in tutta l'UE) pratiche come la manipolazione subliminale dannosa e lo sfruttamento delle vulnerabilità delle persone (ad esempio lo stato di lutto). Obblighi di Trasparenza: i sistemi che generano contenuti sintetici (come gli avatar o i deepfake) devono essere chiaramente etichettati, informando gli utenti che stanno interagendo con una macchina. Queste norme entreranno pienamente in vigore nell'agosto 2026. L'IA Act stabilisce un sistema di vigilanza per garantire il rispetto delle norme e l'applicazione delle sanzioni:

Autorità competenti: L'Ufficio europeo per l'IA e le autorità nazionali degli Stati membri sono responsabili della supervisione e dell'applicazione della legge. Segnalazione incidenti**:** I fornitori e gli operatori sono obbligati a segnalare incidenti gravi e malfunzionamenti alle autorità di vigilanza. Strumenti per i cittadini: È previsto uno "strumento informatore" che consente alle persone di presentare reclami in caso di violazioni. Autorità di Vigilanza. In Italia, la supervisione e l'applicazione delle norme sull'IA sono affidate alle autorità nazionali di vigilanza del mercato (come il Garante per la protezione dei dati personali) in coordinamento con l'Ufficio europeo per l'IA. È previsto inoltre uno "strumento informatore" che consente ai cittadini di presentare reclami in caso di violazione dell'IA Act. **9. Ermeneutica Costituzionale: identità digitale come diritto inviolabile, IA Act e Articolo 2-terdecies del Codice Privacy**

I diritti inviolabili della nostra Costituzione, pur non essendo tutti elencati letteralmente nel testo del 1948, trovano il loro fondamento nell'Articolo 2, inteso dalla dottrina come una "fattispecie aperta", capace di accogliere nuovi bisogni di tutela. Tra i principali diritti figurano: la dignità umana, il diritto alla riservatezza, l'identità personale, il diritto alla vita e il principio di uguaglianza (Art. 3 Cost.). In base al criterio costituzionale, il riconoscimento del diritto alla riservatezza e all'identità personale non trova un riferimento esplicito nel testo del 1948, ma è frutto di un'interpretazione evolutiva dell'art. 2 Cost. come "fattispecie aperta". La dignità umana, pietra angolare della nostra Carta e della Carta di Nizza, deve rappresentare il fine ultimo dello sviluppo tecnologico, escludendo che la macchina possa sostituirsi integralmente all'uomo in valutazioni che attengono alla sua essenza morale. In particolare, l'uso di avatar nei contesti educativi o valutativi deve essere bilanciato con il principio di uguaglianza (art. 3 Cost.), prevenendo i bias di rappresentazione e le discriminazioni algoritmiche che tendono a marginalizzare le minoranze e che, operando in modo opaco, rischiano di creare nuovi pregiudizi sociali, svuotando di fatto il diritto all'identità personale della sua sostanza democratica.

L'Intelligenza Artificiale può intaccare questi diritti in diversi modi:

1. Lesione della Dignità e dell'Identità Personale

CamminoDiritto.it
ISSN 2421-7123

L'IA può essere utilizzata per creare simulacri digitali (avatar o deepfake) che distorcono la narrativa e la reputazione di una persona.

Esempio: la creazione di contenuti sintetici che attribuiscono a un individuo azioni o dichiarazioni mai compiute offende la dignità e l'integrità morale del soggetto. Impatto postumo: l'uso di deadbots per scopi commerciali contrari ai valori del defunto (come il caso dell'attore cinematografico Bruce Lee usato per pubblicizzare alcolici) è considerato una violazione della memoria e della dignità postuma. 2. Violazione del Principio di Uguaglianza (Art. 3 Cost.)

L'uso di algoritmi opachi può introdurre bias algoritmici (pregiudizi) che portano a discriminazioni sistematiche.

Esempio nel settore giudiziario: programmi disegnati per prevedere la recidiva dei detenuti possono basarsi su dati "contaminati" (come l'origine etnica o il livello educativo), portando a decisioni che penalizzano ingiustamente certi gruppi sociali. Esempio sanitario: sistemi di IA che determinano l'accesso alle cure basandosi su criteri di efficienza o profitto rischiano di creare una "medicina per i ricchi", escludendo i più fragili e violando il diritto alla salute. 3. Minaccia al Diritto alla Vita e alla Libertà

Armi autonome: lo sviluppo di sistemi d'arma letali (LAWS), che decidono autonomamente di togliere la vita senza controllo umano, rappresenta una sfida drammatica alla santità della vita e alla responsabilità morale. Sorveglianza e Privacy: l'IA permette un controllo costante e invasivo della vita interiore, riducendo gli spazi di autodeterminazione, e minacciando persino la libertà religiosa attraverso la sorveglianza digitale. Sebbene la giurisprudenza specifica sugli avatar sia in evoluzione, l'ordinamento italiano partendo anche dai preuspposti costituzionali ,ha risposto con importanti novità:

Legge 132/2025: ha introdotto l'Articolo 612-quater c.p., che punisce la diffusione illecita di contenuti falsificati tramite IA idonei a indurre in inganno o causare danno. Articolo 2-terdecies del Codice Privacy: permette di proteggere i dati dei defunti da usi impropri o deformazioni algoritmiche, garantendo il "diritto di divieto" dell'interessato espresso in vita. In sintesi, la sfida attuale è garantire che l'essere umano rimanga al centro del processo decisionale (principio dello human in the loop) affinché la tecnologia non si sostituisca all'individuo in valutazioni morali essenziali.

10. L'Articolo 2-terdecies del Codice Privacy (D.Lgs. 196/2003)

L'inquadramento sistematico dell'Art. 2-terdecies del Codice Privacy. L'ordinamento

CamminoDiritto.it
ISSN 2421-7123

italiano si pone all'avanguardia con l'Art. 2-terdecies del Codice Privacy, che disciplina i diritti dei defunti in conformità alla delega prevista dal Considerando 27 del GDPR. Attraverso un criterio sistematico, la norma coordina la protezione dei dati con la successione ordinaria: mentre i beni digitali economici (criptoattività, NFT) seguono le regole del Codice Civile, i dati personali sono accessibili agli eredi solo in presenza di un "interesse proprio" o di "ragioni familiari meritevoli di protezione". Tuttavia, l'interessato può esercitare il "diritto di divieto" in vita, impedendo l'accesso postumo ai propri dati con una dichiarazione scritta specifica. La dottrina rileva come questo equilibrio miri a preservare la "narrativa della persona" e il suo diritto all'oblio, impedendo deformazioni postume della reputazione.

L'Italia, pertanto, è considerata all'avanguardia grazie all'introduzione dell'Articolo 2-terdecies del Codice Privacy (D.Lgs. 196/2003). Nell'ordinamento italiano, il consenso espresso in vita ha un impatto determinante. Secondo l'Articolo 2-terdecies del Codice Privacy, i diritti sui dati personali di un defunto possono essere esercitati dai superstiti (eredi o chi ha un interesse meritevole), a meno che l'interessato non lo abbia espressamente vietato.

Requisiti del divieto: Per essere valido, il diniego deve essere una dichiarazione scritta, specifica, libera e informata, presentata o comunicata al titolare del trattamento. Revocabilità: L'interessato può revocare o modificare questo divieto in qualsiasi momento della sua vita. Limiti al divieto: Anche se esiste un divieto, questo non può pregiudicare i diritti patrimoniali di terzi o il diritto di difendere i propri interessi in giudizio. Secondo la norma, i diritti sui dati del defunto possono essere esercitati da:

chi ha un interesse proprio: ad esempio un erede o un legatario. chi agisce a tutela dell'interessato: in qualità di suo mandatario o esecutore testamentario. chi ha ragioni familiari meritevoli di protezione: come il coniuge, i figli o i genitori che desiderano preservare la memoria del caro estinto. Principali distinzioni contenute:

Diritti degli eredi: La norma stabilisce che i diritti ex artt. 15-22 del GDPR (accesso, rettifica, cancellazione/oblio) possono essere esercitati da chi ha un interesse proprio, agisce a tutela dell'interessato come mandatario, o per ragioni familiari meritevoli di protezione

Diritto di divieto: L'interessato può vietare in vita l'esercizio di tali diritti con una dichiarazione scritta specifica, libera e informata presentata al titolare del trattamento. Tale divieto non può però pregiudicare i diritti patrimoniali di terzi o il diritto di difesa in giudizio. Un pilastro importante del sistema è, pertanto, il diritto di divieto: l'interessato può impedire preventivamente l'accesso postumo ai propri dati tramite una dichiarazione

CamminoDiritto.it
ISSN 2421-7123

scritta che deve essere specifica, libera e informata. Tuttavia, tale diniego incontra limiti precisi e invalicabili, non potendo pregiudicare i diritti patrimoniali di terzi o il diritto di difesa in sede giudiziaria. Questo equilibrio normativo mira a preservare la "narrativa della persona" e a proteggere la reputazione del de cuius da possibili usi indebiti o deformazioni algoritmiche operate dagli eredi o dalle piattaforme

Tipologia di diritti esercitabili dagli eredi

Gli eredi possono esercitare i diritti previsti dagli articoli da 15 a 22 del GDPR, che includono:

Diritto di accesso: ottenere copia dei dati conservati nelle piattaforme (foto, documenti, email). Diritto di rettifica: correggere informazioni inesatte riguardanti il defunto. Diritto alla cancellazione (Diritto all'oblio): richiedere la rimozione di dati o account non più necessari. Diritto alla limitazione del trattamento e di opposizione: opporsi a determinati utilizzi dei dati del defunto da parte delle aziende. Diritto alla portabilità: trasferire i dati da un servizio a un altro. **11. Profili penali e sanzioni: La Legge 132/2025 e precedenti storici**

L'introduzione dell'art. 612-quater c.p. (L. 132/2025) colma una lacuna normativa punendo la diffusione illecita di contenuti falsificati tramite IA idonei a indurre in inganno. Il legislatore ha riconosciuto l'insidiosità del mezzo tecnologico inserendo un'aggravante generale per i reati commessi mediante sistemi di IA (art. 61 n. 11-decies c.p.), a tutela della fede pubblica e della dignità individuale. La nuova Legge italiana sull'IA (L. 132/2025), pertanto, ha introdotto l'Articolo 612-quater c.p., che punisce con la reclusione da 1 a 5 anni la diffusione illecita di contenuti (immagini, video, voci) falsificati o alterati tramite IA idonei a indurre in inganno o cagionare danno. È prevista anche un'aggravante generale (Art. 61 n. 11-decies c.p.) per qualsiasi reato commesso mediante l'impiego insidioso di sistemi di IA.

In Italia, purtroppo, abbiamo avuto un tragico precedente storico e giuridico, di una giovane ragazza che si tolse la vita per contenuti personali pubblicati in rete; quell'evento tragico che scosse tutta l'opinione pubblica, spinse il legislatore ad intervenire su temi come il "diritto all'oblio" e la tutela della dignità digitale, temi che oggi trovano una nuova e urgente declinazione proprio a causa dell'Intelligenza Artificiale.

Il caso riguardava la diffusione non consensuale di video reali. Oggi, l'IA permette di creare contenuti sintetici altrettanto lesivi (come i deepfake porn). Per colmare questa lacuna, la Legge 132/2025, ha introdotto l'Articolo 612-quater c.p., che punisce con la reclusione da 1 a 5 anni la diffusione di contenuti falsificati o alterati tramite IA idonei a

CamminoDiritto.it
ISSN 2421-7123

indurre in inganno o a causare un danno alla vittima. Il legislatore ha riconosciuto che l'uso dell'IA aumenta l'insidiosità del reato, prevedendo un'aggravante generale (art. 61 n. 11-decies c.p.). Uno dei problemi centrali del caso fu la persistenza dei contenuti in rete dopo la morte della ragazza. L'Italia è oggi all'avanguardia con l'Articolo 2-terdecies del Codice Privacy, che permette agli eredi o a chi ha un "interesse meritevole" di esercitare i diritti del defunto, tra cui il diritto alla cancellazione (oblio) e la rettifica di informazioni inesatte o lesive. Questo strumento mira a preservare la "narrativa della persona" e a impedire che simulacri digitali o contenuti sintetici ne distorcano la reputazione postuma

12. Il vuoto normativo e il "consenso per impostazione predefinita"

Senza istruzioni esplicite, si cade spesso in una "trappola del consenso predefinito". Molti ritengono che la privacy sopravviva alla morte, ma legalmente, in assenza di un divieto scritto, gli eredi potrebbero sentirsi autorizzati a caricare anni di corrispondenza privata in un modello IA per creare un griefbot.

Consenso degli eredi vs. interessato: Esiste una distinzione netta tra l'autorizzazione data dagli eredi (che agiscono come guardiani) e il consenso dell'interessato. Se il defunto non ha autorizzato la creazione di "nuovo" contenuto sintetico in suo nome, l'azione degli eredi potrebbe essere considerata una violazione della dignità postuma. Trasparenza delle piattaforme: L'IA Act europeo (in vigore dal 2026) imporrà obblighi di trasparenza, obbligando i fornitori di deepfake e avatar a informare gli utenti che stanno interagendo con una simulazione, indipendentemente dal consenso ricevuto. **13**. **L’eredità digitale**

Il concetto di eredità digitale si riferisce all'insieme di risorse, sia offline che online, che appartengono a un individuo al momento della sua morte. Questo patrimonio non comprende solo beni materiali, ma una complessa varietà di dati e diritti digitali che richiedono un inquadramento giuridico specifico, distinguendo tra il loro valore affettivo e il loro valore economico.

1. Classificazione del patrimonio digitale

Il patrimonio digitale può essere suddiviso in due macro-categorie principali basate sulla natura dei beni:

Beni a carattere patrimoniale (Beni economici): Sono risorse che possiedono un valore economico intrinseco e quantificabile. Includono: Criptoattività: Criptovalute (come Bitcoin o Ethereum), utility tokens e security tokens. NFT (Non-Fungible Tokens): Certificati digitali di proprietà di beni unici, spesso legati alla crypto art. Virtual Real

CamminoDiritto.it
ISSN 2421-7123

Estate: Terreni e immobili acquistati all'interno dei metaversi. Asset professionali: Fotografie scattate da professionisti, video di registi, testi inediti di autori o nomi a dominio. Account finanziari**:** Crediti su piattaforme di e-commerce o account di pagamento elettronico. Beni a carattere personale: Risorse prive di valore economico diretto, ma dotate di un forte valore morale o affettivo, come e-mail, messaggi WhatsApp, profili social,foto e video amatoriali o diari digitali. **2. Differenze nella qualificazione giuridica**

In Italia, la gestione di questi beni segue binari normativi differenti a seconda della loro natura:

Dati Personali (Art. 2-terdecies del Codice Privacy): I diritti sui dati personali (accesso, rettifica, cancellazione) sono protetti dalla normativa sulla privacy. Gli eredi possono esercitare tali diritti per ragioni familiari meritevoli di protezione, a meno che il defunto non lo abbia espressamente vietato in vita. Beni Digitali Economici (Codice Civile): I beni con valore economico rientrano nella successione ordinaria. Essi sono trattati come asset finanziari e si trasmettono agli eredi secondo le regole del Codice Civile, proprio come un conto corrente o un immobile. **3. Problematiche legate alla titolarità e alle licenze**

Un ostacolo rilevante alla trasmissione ereditaria è rappresentato dalla distinzione tra proprietà e licenza d'uso. Molti beni digitali come e-book, film, brani musicali o videogiochi non sono "acquistati" in senso tecnico, ma concessi in licenza per la durata della vita dell'utente o dell'account. Spesso le clausole contrattuali dei provider vietano il trasferimento mortis causa di questi contenuti, trasformando l'acquisto in un noleggio a lungo termine che si estingue con il titolare.

4. Strumenti di gestione e pianificazione

Per garantire che i beni economici e affettivi non vadano perduti o restino inaccessibili, sono necessari strumenti di pianificazione:

Testamento Digitale: Consente di disporre dei propri beni digitali e di nominare un esecutore digitale incaricato di gestire o cancellare gli account. Mandato post-mortem exequendum: Un contratto con cui si incarica una persona di fiducia di compiere attività materiali (come la consegna di password) dopo il decesso. Soluzioni dei Provider: Strumenti come il "Contatto erede" di Apple o la "Gestione account inattivo" di Google permettono di decidere in anticipo chi potrà accedere ai dati. Digital Maintenance Trust: Una proposta per allocare fondi specifici destinati a coprire i costi di manutenzione dei server e dei cloud dove risiedono i beni digitali, evitandone la cancellazione per

CamminoDiritto.it
ISSN 2421-7123

insolvenza. **14. La violazione dell'integrità della persona postuma**

Il concetto di danno postumo alla reputazione rappresenta una delle frontiere più complesse del diritto nell'era dell'intelligenza artificiale, poiché mette in discussione il principio classico secondo cui i diritti della personalità si estinguono con la morte biologica. Mentre la visione tradizionale epicurea sostiene che il defunto non possa essere danneggiato in quanto non più "soggetto esperiente", la dottrina moderna, guidata da pensatori come Joel Feinberg, riconosce che la "narrativa di una persona**"** e i suoi interessi reputazionali continuino a esistere e meritino protezione.

Il danno alla reputazione postuma si manifesta principalmente quando una replica digitale (deadbot o avatar) distorce l'essenza dell'individuo.

Attribuzione di falsi contenuti: I sistemi di IA generativa possono far dire o fare all'avatar cose che il defunto non avrebbe mai approvato, violando la sua dignità e integrità morale. Deformazione algoritmica: A causa di bias intrinseci o dati frammentari, l'IA può creare una "caricatura" o una versione stereotipata del defunto (effetto "specchio deformante"), riducendo la complessità di una vita a pattern comportamentali mediocri o errati. Sfruttamento commerciale indebito: L'uso dell'immagine postuma per scopi pubblicitari contrari ai valori del defunto (come il caso di Bruce Lee usato per pubblicizzare alcolici nonostante fosse astemio) è considerato una grave offesa alla sua memoria e reputazione.
15. La necessità di " Genuine Presence Assurance"

Per contrastare l'uso di avatar fraudolenti, le fonti indicano come vitale, l'adozione di tecnologie di Genuine Presence Assurance. Questi sistemi non si limitano a verificare che il volto corrisponda ai dati registrati, ma assicurano che l'utente sia:

una persona reale: distinguendo tra un essere umano e una riproduzione digitale o fisica (come un avatar su uno schermo o una maschera). fisicamente presente "ora": impedendo l'iniezione di flussi video pre-registrati o sintetici durante il processo di autenticazione. Il furto d'identità dei defunti (cyber-ghosting) è un rischio crescente, poiché, le protezioni dei dati personali spesso non cessano con la morte. Un avatar di una persona scomparsa potrebbe essere utilizzato per tentare di riattivare o utilizzare credenziali SPID per scopi fraudolenti, come riscuotere indebitamente pensioni o accedere a beni ereditari.

In sintesi, il riconoscimento facciale per lo SPID, deve evolversi parallelamente alla qualità degli avatar, passando da una semplice comparazione d'immagine a una verifica complessa della presenza fisica genuina per evitare che la nostra identità amministrativa venga assorbita da simulacri digitali.

CamminoDiritto.it
ISSN 2421-7123

16. Verso nuovi diritti fondamentali: disclosure, spiegazione e controllo umano

Il termine disclosure (spesso tradotto come "informativa" o "comunicazione dei dati") assume significati specifici a seconda del contesto giuridico, finanziario o tecnologico in cui viene utilizzato, ma il denominatore comune è la trasparenza informativa.

1. Ambito Finanziario e Societario

In termini finanziari, la disclosure è l'azione di rendere disponibili al pubblico tutte le informazioni pertinenti su un'attività commerciale in modo tempestivo.

Scopo: permettere agli investitori di prendere decisioni informate, ridurre l'incertezza del mercato, evitare crisi economiche e contrastare fenomeni come l'insider trading. Contenuto: include fatti, cifre, date, innovazioni e rischi (ESG - ambientali, sociali e di governance) che potrebbero influenzare il valore di un titolo. Regolazione: è strettamente regolata da enti come la SEC negli Stati Uniti o la FCA nel Regno Unito. 2. Ambito Legale e Processuale (Civil Discovery)

Nel diritto processuale civile (particolarmente negli USA e ora anche in parte della legislazione californiana con la SB 235), la disclosure si riferisce allo scambio obbligatorio di informazioni prima del processo.

Initial Disclosures: le parti devono fornire nomi di testimoni, copie di documenti rilevanti e calcoli dei danni senza attendere una richiesta formale della controparte. Obiettivo: evitare "tattiche a sorpresa", snellire le questioni processuali e ridurre i costi della controversia. 3. Ambito Immobiliare (Real Estate)

Nelle transazioni immobiliari, la disclosure è l'obbligo legale del venditore di rivelare fatti materiali (difetti latenti, pericoli ambientali o vincoli legali) che non sono facilmente osservabili dal compratore.

Supera il principio storico del caveat emptor ("compri il compratore a proprio rischio"), proteggendo l'acquirente da perdite di valore inaspettate. 4. Intelligenza Artificiale e Nuove Tecnologie

Nel contesto dell'IA Act e del dibattito etico moderno, la disclosure assume una dimensione di tutela della dignità umana:

CamminoDiritto.it
ISSN 2421-7123

AI Disclosure: è il diritto dell'utente di conoscere la natura artificiale del proprio interlocutore. I fornitori di sistemi di IA (come avatar o deepfake) hanno l'obbligo di etichettare chiaramente i contenuti sintetici. Trasparenza algoritmica: Include il diritto alla spiegazione, ovvero ricevere informazioni sulla logica dei processi decisionali automatizzati per superare l'opacità delle cosiddette "scatole nere" (black-box). 5. Privacy e Pubblica Amministrazione

Nelle leggi sulla privacy (come il Privacy Act del 1974), la disclosure è definita come il permettere l'accesso, il rilascio o il trasferimento di informazioni di identificazione personale (PII) a terzi. In questo caso, la disclosure è spesso vietata senza il consenso scritto dell'interessato.

La dottrina internazionalistica e costituzionale propone la costruzione di tre "nuovi diritti" fondamentali per l'era algoritmica:

Diritto alla AI Disclosure: il diritto di conoscere la natura artificiale dell'interlocutore. Diritto alla spiegazione: il diritto a ricevere informazioni significative sulla logica dei processi decisionali automatizzati, superando l'opacità della "black-box". Diritto allo human in the loop: la garanzia di un controllo umano effettivo e non meramente formale su ogni decisione che incida sui diritti fondamentali (c.d. riserva di umanità). **17. "Magnifica Humanitas": l'intelligenza artificiale nel solco della Dottrina Sociale**

Un contributo determinante al dibattito etico e giuridico contemporaneo giunge dalla prima enciclica di Leone XIV, la "Magnifica Humanitas" (25 maggio 2026), dedicata specificamente alla custodia della persona nel tempo dell'IA. Il Pontefice inserisce idealmente il documento nel solco tracciato da Leone XIII nel 1891 con la "Rerum Novarum": se quest'ultima affrontava le trasformazioni della rivoluzione industriale e la questione operaia, Leone XIV si misura oggi con la rivoluzione digitale dominata da algoritmi e automazione cognitiva. L'enciclica Magnifica Humanitas di Leone XIV, e gli interventi di Papa Francesco, sottolineano come la "disclosure" non è solo un obbligo tecnico, ma un dovere morale per garantire una "ecologia della comunicazione". La trasparenza deve riguardare la progettazione stessa degli algoritmi, rivelando quale idea di persona è inscritta nei dati, per evitare manipolazioni e garantire che la tecnologia sia al servizio del bene comune. Il Papa, quindi, sottolinea con veemenza letterale, che la tecnologia non è neutrale, poiché "assume il volto di chi la pensa, la finanzia e la usa". Il confronto con la Rerum Novarum evidenzia un'urgenza analoga: allora si difendeva la dignità del lavoratore dai telai meccanici, oggi la si difende dalla concentrazione del potere digitale nelle mani di pochi monopolisti tech. Leone XIV richiama la necessità di una "algoretica" e di "disarmare l'IA" per impedire che la sovranità tecnologica surclassi quella democratica e che la persona sia ridotta a mero dato o funzione algoritmica

CamminoDiritto.it
ISSN 2421-7123

18. Riflessioni conclusive

L'immortalità digitale non è più fantascienza, ma una realtà industriale che necessita di una regolamentazione transnazionale armonizzata. La sfida del prossimo decennio sarà bilanciare il desiderio umano di non essere dimenticati con la necessità psicologica di permettere ai morti di riposare e ai vivi di procedere oltre. La tecnologia deve servire come ponte verso il ricordo, non come sostituto dell'assenza, garantendo che la dignità umana non venga sacrificata sull'altare del profitto delle Big Tech.

L'intersezione tra l'immortalità digitale e la psicologia del lutto rappresenta uno dei campi di studio più critici della modernità. L'evoluzione tecnologica ha trasformato la memoria da un archivio passivo (foto, video) in un'entità interattiva (griefbots, avatar), ridefinendo radicalmente il modo in cui gli esseri umani affrontano la perdita.

Il diritto sta tentando di rispondere a queste sfide attraverso diverse strategie:

Tutela dei familiari come "guardiani": In ordinamenti come quello italiano (Art. 2-terdecies Codice Privacy) e brasiliano (Artt. 12 e 20 del Codice Civile), i familiari non sono "proprietari" dei diritti del defunto, ma agiscono come custodi della sua memoria, con il potere di inibire usi che ne pregiudichino l'onore o la reputazione. Diritto d'autore e protezione morale: La legge italiana sul diritto d'autore (L. 633/1941) permette ai familiari di rivendicare la paternità dell'opera e opporsi a qualsiasi deformazione o modifica che rechi pregiudizio all'onore dell'autore defunto. Leggi specifiche sui deepfake: Nuove normative, come quelle della California (AB 1836), vietano esplicitamente l'uso di repliche digitali non autorizzate di artisti defunti, proteggendo sia il valore commerciale che la dignità dell'immagine. Ma cosa manca ancora nel nostro diritto? Nonostante l'Articolo 2-terdecies ponga l'Italia all'avanguardia, mancano ancora diversi elementi per arginare i rischi del fenomeno:

Distinzione tra uso affettivo e commerciale: Attualmente, se non esiste un divieto scritto del defunto, gli eredi possono caricare l'intera corrispondenza privata in un modello IA. Manca una norma che impedisca ai familiari, pur agendo come "guardiani", di trasformare il ricordo in uno sfruttamento commerciale non autorizzato o in una "dipendenza algoritmica". Protocolli di Cybersecurity Post-Mortem: Una volta terminata la vita biologica, cessano le protezioni del GDPR. Manca uno standard nazionale per la gestione sicura dell'eredità digitale che protegga i dati dei defunti dal ghosting (furto d'identità per frodi bancarie o assicurative). Linee Guida del Garante: L'Articolo 2-terdecies è considerato "eccessivamente vago" e mancano ancora linee guida operative che definiscano come presentare le dichiarazioni di divieto ai titolari del trattamento in modo

CamminoDiritto.it
ISSN 2421-7123

uniforme. Formalismo del Testamento Digitale: Non esiste una procedura semplificata e legalmente riconosciuta (come il Digital Will statunitense o la tecnologia blockchain con valore probatorio) per depositare le volontà digitali e le chiavi di accesso ai wallet di criptovalute o account social in modo sicuro e segreto. Sanzioni Specifiche per la Decezione: Manca un apparato sanzionatorio per le aziende che utilizzano avatar di defunti per manipolare emotivamente i superstiti a scopi di marketing, andando oltre la semplice violazione della privacy per toccare il danno alla dignità. Tecnicamente, per arginare i rischi dell'affidamento dei nostri dati all'IA, invece, occorrerebbe affidarsi ai Model Context Protocol (MCP). Il MCP è uno standard aperto introdotto (principalmente da Anthropic) per consentire alle intelligenze artificiali di connettersi in modo sicuro e standardizzato a sorgenti di dati esterne e strumenti. L'MCP potrebbe rappresentare l'infrastruttura tecnica per risolvere alcuni dei problemi discussi di approvvigionamento di dati sensibili, perchè protetti e analizzati attraverso questo sistema di controllo. L'MCP standardizza il modo in cui l'IA accede ai dati, potenzialmente offrendo criteri di permessi più granulari che potrebbero essere integrati nei "testamenti digitali" per limitare cosa l'IA può o non può consultare. L'MCP, in sintesi, è lo strumento tecnico che potrebbe rendere quel processo di "attivazione dei dati" molto più fluido e interconnesso. La sfida per le aziende, attualmente, è dotarsi di apparati di IA in grado di poter trasmettere dati reali agli MCP, in maniera sicura per tutti. I prompt richiesti attraverso i MCP, saranno in grado di orientare le scelte, gli MCP avranno un potere decisionale nell'orientare le scelte finite degli utenti che faranno loro affidamento per la selezione in determinati ambiti. Infine, potremmo anche giungere che siamo di fronte al rischio di una nuova "questione operaia 2.0", dove la tecnologia non viene usata per migliorare il lavoro, ma per dequalificare il lavoratore o sostituirlo completamente in nome dell'efficienza, riducendo l'essere umano a mero "ingranaggio" o funzione algoritmica. Il diritto sta correndo per colmare questi vuoti, cercando di impedire che il simulacro (l'avatar) possa operare in modo autonomo nello spazio legale e amministrativo senza un effettivo controllo umano.

In conclusione, l'immortalità digitale richiede un passaggio da una tutela puramente repressiva a una governance proattiva della dignità umana. Il diritto deve garantire che la tecnologia serva come ponte verso il ricordo e non come simulacro sostitutivo dell'assenza, assicurando che la "misura di tutte le cose".

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

1. WARREN S. – BRANDEIS L., The Right to Privacy, in Harvard Law Review, vol. 4, n. 5, 1890, pp. 193-220.

2. WEIZENBAUM J., ELIZA - A Computer Program For the Study of Natural Language Communication Between Man and Machine, in Communications of the ACM, vol. 9, n. 1, 1966, pp. 36-45.

3. REGOLAMENTO (UE) 2016/679 del Parlamento europeo e del Consiglio (GDPR), in particolare il Considerando 27 relativo ai dati delle persone decedute.

4. REGOLAMENTO (UE) 2024/1689 del Parlamento europeo e del Consiglio (Artificial Intelligence Act – IA Act).

5. D.LGS. 30 GIUGNO 2003, N. 196 (Codice in materia di protezione dei dati personali), Art. 2-terdecies (Diritti riguardanti le persone decedute).

6. LEGGE 17 MAGGIO 2025, N. 132 (Disposizioni in materia di intelligenza artificiale), con particolare riferimento all'introduzione dell'art. 612-quater c.p. e dell'aggravante di cui all'art. 61 n. 11-decies c.p..

7. LEONE XIV, Lettera Enciclica Magnifica Humanitas sulla custodia della persona umana nel tempo dell'Intelligenza Artificiale, 25 maggio 2026.

8. LEONE XIII, Lettera Enciclica Rerum Novarum sulle condizioni degli operai, 15 maggio 1891.

9. DICASTERO PER LA DOTTRINA DELLA FEDE – DICASTERO PER LA CULTURA E L'EDUCAZIONE, Nota Antiqua et nova sul rapporto tra intelligenza artificiale e intelligenza umana, 28 gennaio 2025.

10. SIGNORELLI A. D., Simulacri digitali. Le allucinazioni e gli inganni delle nuove tecnologie, ADD editore, 2025.

11. SISTO D., La morte si fa social. Immortalità, memoria e lutto nell'epoca della cultura digitale, Bollati Boringheri, 2018.

12. IACONO G., Le sfide della società onlife. I rischi della rivoluzione digitale e le competenze indispensabili per affrontarla, Franco Angeli, 2023.

13. COSETTA M., Memoria eterna, Bruno Editore, 2025.

14. POMA L., Il sex appeal dei corpi digitali. Seduzione, amori, tradimenti, malattie e immortalità dei nostri digital body, Franco Angeli, 2016.

15. REITZ K., The Digital Afterlife: Immortality in the Cloud, 2026.

16. SILVA A. P., Who Owns the Dead? Digital Replicas and Posthumous Personality Rights, 2026.

17. DEEPBRAIN AI, Re;memory - Analisi dei costi e impatto sociale.

18. WIKIPEDIA, voci Digital Immortality e ELIZA Effect.

19. TOGA, Codice della Privacy, Art. 2-terdecies.

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina: https://rivista.camminodiritto.it/articolo.asp?id=11807