Persona e Identità Digitale

Dignità, responsabilità e cura nella società algoritmica



Via Aurelia, 796 | 00165 Roma | +39 06 68 19 25 54 | segreteria@scienzaevita.org | www.scienzaevita.org

Persona e Identità Digitale

Dignità, responsabilità e cura nella società algoritmica

Redattrici principali: Dott.ssa Maria Teresa Iannone, Prof.ssa Giovanna Costanzo

Indice dei Contenuti

Introduzione
1. Identità digitale e persona: la trasformazione dell'umano nell'infosfera
1.1 La trasformazione digitale dell'identità
1.2 Primo mutamento: dalla persona all'organismo informazionale
1.3 Secondo mutamento: l'identità digitale come nuova condizione dell'umano
1.4 Identità personale e identità digitale: tra continuità e rottura
1.5 Algoritmi, profilazione e frammentazione del sé
1.6 Autonomia della persona nell'era digitale?
2. Infrastrutture, potere e soggetto politico: identità digitale e democrazia
2.1 L'infrastruttura invisibile dell'identità digitale: modelli transazionali, quadri di fiducia e limiti strutturali
2.1.1 Attori e quadri di fiducia: la persona mediata
2.1.2 Identità federata e moltiplicazione dei profili
2.2 Implicazioni per la persona e la democrazia
2.3 Identità digitale, persona e democrazia: il problema del soggetto politico nell'era dell'infosfera
3. Diritto, responsabilità e governance dell'identità digitale
3.1 Identità digitale e tutela della persona: diritti e responsabilità
3.2 Regolamentazione e governance
3.2.1 La necessità di una governance dell'innovazione
3.2.2 Le sfide del Diritto nel controllo dell'innovazione tecnologica
3.3 Modelli di governance etica per un uso responsabile: trasparenza, controllo e responsabilità
4. Identità digitale nella società algoritmica: decisioni automatizzate, servizi e sanità
4.1 Dalla società industriale alla società algoritmica
4.2 Il potere predittivo degli algoritmi, automazione e controllo
4.2.1 Il potere predittivo degli algoritmi e il rischio di determinismo
4.2.2 Automazione, decisione e responsabilità
4.2.3 La questione del controllo umano sulle decisioni e la dipendenza dagli algoritmi

4.3 L'impatto delle tecnologie sui servizi e sulla cura
4.3.1 Innovazione tecnologica e miglioramento dei servizi
4.3.2 Efficienza, prevenzione e qualità della vita
4.3.3 Il ruolo della tecnologia nelle relazioni
4.4 L'identità digitale in ambito sanitario
5. Cura, dignità ed etica della progettazione: custodire l'umano
5.1 Custodire l'umano e le nuove sfide etiche
5.2 La crisi dell'etica nell'era digitale
5.3 Etica della progettazione e dignità della persona
5.3.1 Identità digitale e potere di definizione
5.3.2 La dignità come fondamento non negoziabile
5.3.3 Narrazione, riconoscimento e responsabilità: l'importanza di un'etica nella progettazione
5.4 Bioetica, tecnica e potere: il rischio della società tecnocratica
5.4.1 Disuguaglianze digitali e ingiustizia algoritmica
5.4.2 Formazione, consapevolezza e cittadinanza digitale
5.4.3 La cura tra tecnica e relazione: contro la deumanizzazione
6. Prospettive future e proposte: verso una coesistenza equilibrata tra cambiamenti digitali e umanità
6.1 Come garantire una coesistenza equilibrata fra cambiamenti digitali e umanità
6.2 Il rischio di limiti etici inefficaci: verso un'etica della resistenza
6.3 Orientamenti per integrare l'identità digitale nel concetto più ampio di persona
6.4 Educazione digitale: formazione critica delle nuove generazioni e alfabetizzazione emotiva
6.5 Il ruolo delle istituzioni, delle università e della società civile

Conclusioni

Riferimenti bibliografici

- ***I documenti di studio del Centro Studi Scienza & Vita propongono una sintesi riassuntiva del lavoro di ricerca, approfondimento e riflessione bioetica che i diversi gruppi di studio svolgono costantemente durante l'anno. Ciascuno di essi è dedicato ad un tema specifico, scelto tra le questioni bioetiche di maggior interesse comune e attualità.***

Introduzione

Il mutamento prodotto dalla rete delle tecnologie dell'informazione e della comunicazione e dai sistemi di intelligenza artificiale ha trasformato profondamente la nostra esistenza e i rapporti che intessiamo con gli altri. Questo capillare cambiamento che ha coinvolto diversi aspetti della vita quotidiana – da quella familiare, a quella lavorativa, a quella dell'intrattenimento – non ha prodotto una semplice evoluzione tecnologica, bensì è diventato un processo che ha trasformato le condizioni antropologiche del vivere: il modo in cui gli esseri umani abitano il mondo, organizzano le loro esperienze e intrecciano relazioni significative.

Siamo dunque di fronte al sorgere di un inedito ambiente di vita, in cui tutto ciò che transita è informazione **(Floridi, 2011)**: non soltanto i documenti che produciamo, i dati che ci scambiamo o le immagini che conserviamo, ma anche gli agenti che vi operano, siano essi esseri in carne e ossa o artefatti digitali, algoritmi, software, intelligenze artificiali. Un *ambiente di vita* paragonabile per funzione alla biosfera – sebbene distinto per struttura e dinamiche – poiché comprende non solo internet o i media digitali, ma l'insieme di tutti i processi informazionali, *online* e *offline*, naturali e artificiali, ai quali tutti partecipano, plasmando un contesto che cresce, si modifica e si rigenera continuamente. Si è avviata così una trasformazione profonda dei processi produttivi e organizzativi della società contemporanea, come pure delle modalità attraverso cui la persona viene compresa, riconosciuta e rappresentata, del modo in cui costruisce relazioni e prende decisioni – anche quando queste riguardano percorsi delicati come quelli del prendersi cura della persona sofferente.

In questo scenario, sistemi algoritmici sempre più sofisticati intervengono in ambiti decisivi della vita individuale e collettiva: dall'accesso ai servizi alla selezione lavorativa, dalla sicurezza alla sanità, fino alle relazioni interpersonali. Le decisioni automatizzate, non sempre immediatamente decifrabili, pongono interrogativi cruciali sul controllo umano, sulla responsabilità e sulla legittimità delle «scelte» operate dalle macchine.

In questa progressiva digitalizzazione della società contemporanea, anche l'*identità digitale* sta diventando una dimensione strutturale dell'esperienza umana, incidendo profondamente sulla comprensione della persona, della sua autonomia e della continuità del sé. Essa ha assunto sempre più una posizione centrale, ponendo dilemmi antropologici ed etici di non poco conto.

Se la persona, intesa come inscindibile unità psichica, spirituale e corporea, ha costituito il punto di riferimento identificante per ciascun essere umano, il rischio che

venga oggi assimilata e «ridotta» a un insieme di meri dati algoritmici rappresenta una preoccupante forma di riduzionismo.

Nel momento in cui si parlasse non più di persona, come nucleo unitario e stabile, ma di un'identità concepita piuttosto come il risultato di una molteplicità di rappresentazioni, dati, profili e inferenze algoritmiche, tale processo – se non vagliato e governato criticamente – potrebbe condurre a una visione funzionalista dell'essere umano. Il valore della persona verrebbe allora misurato sulla base della sua tracciabilità, prevedibilità ed efficienza. Confrontando, inoltre, questo concetto con quello di identità personale, si aprono ulteriori questioni.

Tradizionalmente, per identità personale si intende il tentativo di rispondere alla domanda «chi sono?», attraverso cui il soggetto si sforza di riconoscersi come un'unicità che permane nel passare del tempo **(Ricœur, 1990)**. L'identità digitale può diventare problematica quando i dati e i profili che rappresentano la persona ne condizionano l'autonomia e la libertà decisionale.

Obiettivo del presente documento è analizzare le trasformazioni di ciò che Floridi ha definito «quarta rivoluzione» **(Floridi, 2014)**, con particolare riguardo all'identità digitale, adottando uno sguardo interdisciplinare che tenga insieme dimensione antropologica, etica e sociale, senza demonizzare la tecnologia, ma interrogandosi sulle condizioni necessarie affinché l'innovazione rimanga realmente al servizio della persona.

Il primo capitolo affronta il cambiamento della rappresentazione di sé quando all'identità personale si sovrappone quella digitale, misurandosi con prospettive filosofiche (Ricœur, Floridi, Han) che mettono in luce le dinamiche di frammentazione, le opportunità di espressione e i rischi di eteronomia che emergono nell'ecosistema digitale contemporaneo.

Il secondo capitolo sposta l'attenzione sulle infrastrutture che rendono operativa l'identità digitale – sistemi di autenticazione, identità federata, quadri di fiducia – e sulle loro implicazioni per la vita democratica: quando l'accesso ai diritti passa attraverso un'architettura tecnica, è in gioco il riconoscimento stesso della persona come soggetto politico.

Il terzo capitolo considera il contesto giuridico in cui ci muoviamo, caratterizzato da una tensione costante fra innovazione tecnologica e tutela dei diritti fondamentali. Quando si parla di identità e della sua frammentazione, infatti, emerge anche una questione giuridica fondamentale: la possibilità che la persona perda il controllo sui dati che la rappresentano, con conseguenze sulla tutela della sua autonomia, della sua autodeterminazione informativa e dei suoi diritti fondamentali.

Il quarto capitolo richiama i tratti essenziali della società algoritmica – il potere predittivo dei sistemi, l'automazione delle decisioni, il problema del controllo umano – come premessa per esaminare l'ambito della cura.

Un'attenzione particolare è infatti riservata al settore sanitario, un ambito emblematico poiché in esso i cambiamenti digitali mostrano al tempo stesso le applicazioni più promettenti e le derive più preoccupanti. La relazione di cura è infatti spazio privilegiato di riflessione sul rapporto tra tecnologie e umanità, tra efficienza e responsabilità, tra sapere scientifico e dimensione umana.

Il quinto capitolo raccoglie queste analisi in una riflessione sull'etica della progettazione, nell'orizzonte bioetico che caratterizza l'intero documento: le scelte tecniche che definiscono un sistema di identità sono già scelte morali, perché stabiliscono chi può essere riconosciuto e a quali condizioni. La dignità della persona e l'etica della cura offrono il criterio per valutarle.

In questo quadro emerge con forza la necessità di un'etica della responsabilità e, al tempo stesso, della resistenza: resistenza alla riduzione della persona a mero oggetto informazionale, alla delega totale alle macchine, alla perdita di senso delle relazioni umane. Solo mantenendo vivo questo orizzonte critico sarà possibile immaginare una coesistenza equilibrata tra umanità e tecnologie. A questo compito sono dedicate le proposte del sesto capitolo e le conclusioni.

1. Identità digitale e persona: la trasformazione dell'umano nell'infosfera

1.1 La trasformazione digitale dell'identità

L'umanità sta attraversando una fase storica caratterizzata da una trasformazione tecnologica senza precedenti, in cui la digitalizzazione pervade ogni ambito dell'esistenza sociale, economica e relazionale. Strumenti e sistemi che fino a pochi decenni fa appartenevano alla sfera della fantascienza sono oggi parte integrante della quotidianità, modificando non solo i comportamenti, ma anche le categorie fondamentali attraverso cui l'individuo comprende sé stesso e il mondo.

Tra le questioni più rilevanti vi è quella relativa all'identità personale. Tradizionalmente studiata dalla filosofia, dalla psicologia, dalla sociologia e dal Diritto come dimensione complessa e stratificata dell'essere umano, l'identità rimanda alla capacità del soggetto di riconoscersi come soggettività unica e distinta, capace di mantenere il nucleo più profondo del sé attraverso il mutare del tempo e delle esperienze **(Ricœur, 1990)**.

Questo concetto viene oggi profondamente riplasmato dall'ambiente digitale. L'emergere dell'identità digitale non rappresenta semplicemente una trasposizione

dell'identità nello spazio virtuale, ma introduce modalità inedite di rappresentazione, riconoscimento e costruzione del sé, che mettono in discussione i tradizionali concetti di unità, continuità e autonomia della persona.

La moltiplicazione delle piattaforme digitali, dei servizi *online* e degli ambienti virtuali produce una proliferazione di identità parziali, spesso non solo slegate tra loro, ma in tensione o conflitto. La domanda centrale, di conseguenza, non è più se l'identità digitale influisca su quella personale (dato ormai evidente), bensì in che modo essa stia ridefinendo la nozione stessa di persona.

1.2 Primo mutamento: dalla persona all'organismo informazionale

Uno degli effetti più significativi della società algoritmica è il rischio di una trasformazione della concezione dell'essere umano. Luciano Floridi ne ha offerto la descrizione più influente: per lui, però, non si tratta di una perdita, ma della condizione nuova in cui l'uomo si trova a vivere.

Nel quadro antropologico personalista qui assunto, l'essere umano è considerato nella sua unità psichica, spirituale e corporea. La riflessione di Merleau-Ponty richiama, in particolare, il carattere incarnato dell'esperienza e il ruolo costitutivo del corpo nel rapporto con il mondo **(Merleau-Ponty, 1945)**. Quando, invece, sono i dati e le informazioni a essere traghettati da un sistema all'altro, anche l'essere umano viene interpretato, nella prospettiva di Floridi, come organismo informazionale, un *inforg* **(Floridi, 2014)**: un essere che vive e agisce nell'infosfera, attraverso relazioni e scambi informativi in cui la dimensione fisica e quella digitale sono strettamente intrecciate. In questa prospettiva, l'essere umano viene descritto attraverso le relazioni informative che intrattiene nell'infosfera, come nodo dinamico di una rete di scambi e interazioni.

Nella prospettiva informazionale di Floridi, essere persone nell'infosfera significa essere *organismi informazionali*: le informazioni personali non sono soltanto qualcosa che possediamo, ma sono costitutive della nostra identità.

Di questa prospettiva il presente documento accoglie la forza descrittiva: essa coglie con precisione il modo in cui, nell'infosfera, le persone vengono rappresentate, raggiunte e trattate. Va però chiarito un punto: Floridi non identifica la persona con i suoi dati digitali e descrive la realtà in termini informativi senza affermare che la realtà sia, in se stessa, informazione. La differenza riguarda il fondamento dell'identità. Per il presente documento esso non sta nelle relazioni informative in cui la persona è inserita, ma nel suo essere, che viene prima dei dati e non si lascia ridurre a essi.

Questa progressiva traduzione dell'esistente in flussi immateriali incrocia una fortissima intuizione della dottrina giuridica italiana. Già alla fine del secolo scorso, Stefano Rodotà **(Rodotà, 1995)** aveva profeticamente intravisto il rischio della nascita di un «corpo elettronico», inteso come scomposizione e duplicazione della persona in

una serie di dati memorizzati nelle banche dati private e pubbliche. La riflessione giuridica sul «corpo elettronico» può essere posta in dialogo con la nozione filosofica di inforg, pur nella diversità dei rispettivi quadri teorici, per interrogarsi sul rapporto tra la persona e le informazioni che la riguardano e sui rischi di una sua riduzione a un insieme di dati.

Nella prospettiva di Floridi, la dimensione informazionale della soggettività assume rilievo anche sul piano etico: tutelare le informazioni personali significa proteggere l'identità e l'integrità della persona. Il rischio di riduzionismo emerge quando la persona viene identificata esclusivamente con i dati che la rappresentano e con le tracce che lascia in rete, trascurando le dimensioni della sua esperienza che non sono traducibili in informazioni digitali. Accentuando la dimensione informazionale e trascurando il riferimento alla corporeità (che rimanda alla dignità e integrità dell'essere umano e alla sua interazione con il contesto) si finisce per misconoscere quella stessa integralità.

La riduzione dell'essere umano a un insieme di dati rischia di favorire una concezione strumentale della persona, valutata in base alla sua utilità, efficienza e prevedibilità: in tale prospettiva, ciò che non è misurabile tende a essere marginalizzato o escluso dai processi decisionali.

1.3 Secondo mutamento: l'identità digitale come nuova condizione dell'umano

Con il crescere del potere del digitale, identità personale e identità informazionale tendono sempre più a sovrapporsi nella rappresentazione sociale e istituzionale della persona; sul piano concreto, esse vengono sempre più spesso trattate come se coincidessero. Se si guarda l'evoluzione tecnologica nel contesto contemporaneo, appare evidente come l'identità digitale si sia progressivamente evoluta da semplice strumento di autenticazione a infrastruttura complessa che comprende dati anagrafici, informazioni biometriche, profili sociali, comportamenti di navigazione, preferenze, relazioni e inferenze algoritmiche. Non si limita a rappresentare l'individuo, ma contribuisce attivamente a definirlo, tanto sul piano sociale quanto su quello istituzionale.

Luciano Floridi **(2015)** descrive con il termine «onlife» una condizione in cui le esperienze *online* e *offline* sono sempre più intrecciate: il digitale non costituisce un ambito separato dalla vita quotidiana, ma ne permea le relazioni, le pratiche e le forme di rappresentazione di sé. In questa dimensione l'identità digitale non è un doppio virtuale privo di conseguenze: produce effetti reali e contribuisce attivamente a definire l'individuo sul piano sociale e istituzionale.

Tuttavia, se l'essere umano si comprende e si dichiara solo attraverso le relazioni informative che intrattiene in rete, si produce una progressiva decentralizzazione dell'identità.

Per Ricœur, l'identità narrativa prende forma nell'intreccio tra il racconto di sé, le relazioni con gli altri e le vicende della propria vita **(Ricœur, 1990)**. Nell'ambiente *onlife*, questa costruzione è ulteriormente mediata da sistemi tecnologici, piattaforme e algoritmi che raccolgono e interpretano dati personali, spesso attraverso processi poco trasparenti. È proprio in questa perdita di co-autorialità narrativa che l'istanza filosofica diventa urgenza giuridica: il soggetto perde il controllo sulle informazioni che lo rappresentano, richiedendo al Diritto nuove forme di tutela dell'autodeterminazione per preservare l'autonomia e la dignità della persona.

1.4 Identità personale e identità digitale: tra continuità e rottura

L'identità personale può essere intesa come l'integrazione dinamica di credenze, emozioni, ricordi, aspirazioni e ruoli sociali che contribuiscono a definire il senso di sé; non è mai unitaria in senso rigido, ma si articola in una pluralità di dimensioni che variano a seconda dei contesti. Questa pluralità non contraddice l'unità della persona richiamata in apertura: tale unità è di ordine ontologico e precede le sue manifestazioni. Proprio perché radicata nell'essere, essa può esprimersi in una pluralità di dimensioni e di ruoli senza dissolversi; l'identità vissuta e narrata **(Ricœur, 1990)** è il modo in cui questa unità si manifesta nel tempo, non ciò che la costituisce. Nella società digitale, al contrario, questa pluralità tende a trasformarsi in frammentazione.

L'identità digitale introduce, infatti, una molteplicità di rappresentazioni del sé che non sempre risultano coerenti tra loro. Ogni piattaforma favorisce una specifica modalità di presentazione: il sé professionale nei contesti lavorativi, il sé estetizzato nei social visivi, il sé polemico nei forum o nelle piattaforme di microblogging. Questa proliferazione di identità parziali costringe l'individuo a gestire narrazioni multiple e spesso disallineate, con il rischio di smarrire un centro unificante.

Secondo Erving Goffman **(Goffman, 1959)**, l'identità ha sempre avuto una dimensione performativa, poiché gli individui mettono in scena ruoli diversi a seconda delle situazioni mediante la maschera. Il digitale amplifica questa dinamica, trasformando la maschera in profilo e rendendo di fatto permanente ciò che, in passato, era circoscritto e contestuale.

1.5 Algoritmi, profilazione e frammentazione del sé

L'elemento distintivo dell'identità digitale contemporanea è la sua dimensione algoritmica. Come osserva Shoshana Zuboff **(Zuboff, 2019)**, l'identità non è più soltanto ciò che l'individuo esprime consapevolmente, ma anche ciò che viene inferito dai sistemi di analisi dei dati. Le piattaforme digitali non si limitano a registrare informazioni, ma producono profili predittivi che influenzano le opportunità, le relazioni e le scelte dell'individuo.

Byung-Chul Han **(Han, 2014)** interpreta questa trasformazione come una forma di potere psicopolitico, in cui la trasparenza e l'auto-esposizione del soggetto ne erodono l'interiorità, trasformandolo in un'entità performativa che si auto-sorveglia e si auto-sfrutta. L'identità digitale, in questo scenario, non è più uno spazio di libertà, ma un dispositivo di ottimizzazione continua che frammenta il sé riducendone profondità e interiorità.

In questo nodo si colloca una questione giuridica fondamentale: la scomposizione della persona in profili statistici riduce la complessità dell'umano a categorie funzionali di controllo, minando alla base l'autodeterminazione informativa del soggetto concreto.

1.6 Autonomia della persona nell'era digitale?

La questione dell'autonomia rappresenta uno dei nodi centrali del rapporto tra identità digitale e persona. In senso kantiano, l'autonomia consiste nella capacità del soggetto di darsi da sé la legge, ovvero di autodeterminarsi razionalmente. Tale definizione va però precisata: nella prospettiva personalista qui assunta l'autonomia non fonda la dignità, ma ne è un'espressione. Essa indica la libertà di una persona costitutivamente in relazione, orientata al bene e radicata in una dignità che la precede e che non dipende dal suo effettivo esercizio. Nell'ecosistema digitale questa capacità è messa alla prova da architetture persuasive, meccanismi di *nudging* e sistemi di personalizzazione che orientano le scelte senza ricorrere a coercizioni esplicite. Il potere, nell'era algoritmica, non si esercita principalmente attraverso la coercizione, bensì attraverso l'orientamento delle scelte, la previsione dei comportamenti e la modulazione delle possibilità. L'autonomia non scompare, ma viene progressivamente condizionata.

Come suggerisce Paul Ricœur **(Ricœur, 1990)**, l'autonomia può tuttavia essere reinterpretata come co-autorialità: la capacità di partecipare attivamente alla costruzione della propria identità narrativa anche in contesti complessi e mediati. In questa prospettiva, l'individuo non è completamente determinato dai sistemi digitali, ma può esercitare pratiche di resistenza, consapevolezza e gestione critica della propria visibilità e dei propri dati. Nelle reti sociotecniche, l'agire umano si intreccia con il funzionamento dei sistemi digitali. Preservare l'autonomia personale richiede quindi competenze etiche e cognitive, oltre alla possibilità concreta di comprendere, valutare e contestare le decisioni che incidono sulla propria vita.

Preservare l'autonomia della persona significa riconoscere la sua capacità critica e relazionale, piuttosto che limitarla alla gestione dei propri dati. L'identità digitale deve restare uno strumento al servizio della persona, non il criterio attraverso cui essa viene definita e governata.

Colta attraverso queste distinzioni, l'identità digitale non rappresenta semplicemente una minaccia, ma una trasformazione profonda. La sfida che ci attende non consiste nel rifiutare la digitalizzazione, ma nel pensare infrastrutture, istituzioni e pratiche

capaci di riconoscere la persona nella sua complessità, preservandone la continuità temporale, l'autonomia morale e la dignità politica. Solo a questa condizione l'identità digitale potrà diventare un fattore di emancipazione, e non un'ulteriore forma di riduzione funzionale dell'essere umano.

Una comprensione piena di queste dinamiche, però, non è possibile senza analizzare anche le infrastrutture invisibili dell'infosfera e le implicazioni che queste hanno per la democrazia digitale.

2. Infrastrutture, potere e soggetto politico: identità digitale e democrazia

2.1 L'infrastruttura invisibile dell'identità digitale: modelli transazionali, quadri di fiducia e limiti strutturali

Accanto alla dimensione simbolica, narrativa e relazionale dell'identità digitale esiste una dimensione meno visibile ma altrettanto decisiva: quella *infrastrutturale e transazionale*[1] che incide profondamente sulla costruzione del sé, sulla sua autonomia e unità e sulla sua partecipazione democratica. È in questa sfera, spesso relegata al linguaggio tecnico o amministrativo, che si giocano alcune delle trasformazioni più rilevanti nel rapporto tra persona, potere e tecnologia.

Nel mondo contemporaneo, l'identità digitale è conosciuta e percepita per lo più come un meccanismo funzionale che consente l'accesso a servizi essenziali: sanitari, educativi, bancari, previdenziali e amministrativi. Essa assume così la forma di ciò che può essere definito identità digitale transazionale: quell'insieme di attributi, credenziali e certificazioni che permettono a un soggetto di essere riconosciuto come avente diritto all'interno di uno specifico sistema. Più difficile è comprendere e avere consapevolezza di come sia diventata anche un dispositivo di espressione e di rappresentazione della persona.

È bene non dimenticare che ogni accezione apparentemente neutra e strumentale comporta in realtà una trasformazione profonda della nozione di persona. Nella logica della identità digitale l'essere umano non viene riconosciuto nella sua interezza, bensì rappresentato come *proxy*, ovvero come un'entità funzionale ridotta a un insieme di dati pertinenti a una determinata funzione/transazione. L'identità, in tal modo, non indica più chi la persona sia, bensì ciò che il sistema richiede che essa sia per poter operare.

[1] L'identità digitale è *infrastrutturale* perché consente l'accesso a servizi e sistemi; è *transazionale* perché viene utilizzata per compiere operazioni, come presentare una domanda o effettuare un pagamento.

2.1.1 Attori e quadri di fiducia: la persona mediata

Nei sistemi di identità federata (un'unica identità per accedere a servizi diversi), come SPID, il processo di accesso ai servizi coinvolge tipicamente tre attori: l'utente, il fornitore del servizio e il gestore dell'identità digitale (*identity provider*), che autentica l'utente e comunica al fornitore del servizio l'esito dell'autenticazione e gli attributi necessari per l'accesso[2]. Questa triangolazione, pur apparendo puramente tecnica, introduce in realtà una mediazione strutturale tra la persona e i suoi diritti.

Il riconoscimento non avviene più direttamente, ma attraverso sistemi di fiducia formalizzati (i cosiddetti *trust frameworks)* che stabiliscono protocolli, responsabilità, livelli di sicurezza e condizioni d'uso. Tali quadri di fiducia, dai sistemi informali della vita quotidiana fino alle architetture digitali complesse come SPID, non sono strumenti neutrali: definiscono chi può essere riconosciuto, a quali condizioni e con quali conseguenze.

Da un punto di vista filosofico-politico, ciò equivale a una ridefinizione del riconoscimento stesso. Se, come insegna Ricœur **(Ricœur, 2004)**, il riconoscimento è una relazione intersoggettiva che attua le reciproche libertà, nel contesto digitale esso viene progressivamente delegato a dispositivi tecnici che operano secondo logiche di efficienza, sicurezza e interoperabilità. Questo tipo di riconoscimento è certamente valido ed efficace nell'ambito delle transazioni e della sicurezza digitale. Tuttavia, la persona rischia di essere riconosciuta non più come soggetto morale, responsabile e autonomo, bensì come mero nodo affidabile di una rete transazionale.

[2] Gli attributi sono le informazioni associate all'identità dell'utente, come nome, codice fiscale o altre caratteristiche richieste dal servizio.

2.1.2 Identità federata e moltiplicazione dei profili

Come si è accennato, la soluzione tecnica dell'identità federata[3], nata dall'esigenza di ridurre la crescente proliferazione di credenziali, è un modello funzionale che consente di riutilizzare un unico sistema di riconoscimento digitale in contesti diversi (ad esempio, lo SPID).

Questo modello semplifica l'accesso a servizi diversi mediante una stessa identità digitale. I rischi di concentrazione del potere informazionale dipendono tuttavia dall'architettura adottata, dal ruolo dei gestori e dalle garanzie che regolano il trattamento dei dati.

Occorre quindi valutare chi risponde degli errori, chi stabilisce i criteri di accesso e quali controlli siano previsti. La federazione può ridurre la proliferazione delle credenziali, ma non elimina necessariamente la pluralità dei profili associati alla persona nei diversi servizi: resta essenziale evitare che tali rappresentazioni parziali compromettano la sua autonomia e la tutela dei suoi diritti.

Ne deriva una conseguenza fondamentale: la molteplicità delle identità digitali non è un'anomalia temporanea, ma una caratteristica strutturale della società digitale. E proprio questa molteplicità, se non governata da una visione antropologica adeguata, rischia di dissolvere la continuità della persona.

2.2 Implicazioni per la persona e la democrazia

Quando l'identità digitale diventa la condizione di accesso ai diritti, la sua architettura non è mai neutrale: determina di fatto chi è visibile, chi è riconoscibile e chi resta escluso.

Una criticità riguarda i cosiddetti «malati invisibili», le cui condizioni non trovano adeguato riconoscimento nei percorsi diagnostici e amministrativi. L'assenza di una diagnosi definita o le difficoltà di classificazione possono ostacolare, fino a impedire, l'accesso a specifiche esenzioni, prestazioni o percorsi assistenziali. Pur restando formalmente riconosciuto, il diritto alla cura può così risultare, di fatto, non esercitabile: la persona conserva la titolarità del diritto, ma si vede preclusa la possibilità concreta di ricevere le cure di cui ha bisogno.

La dimensione transazionale dell'identità digitale si intreccia così direttamente con la tutela e l'effettiva fruizione dei diritti sanitari dei singoli cittadini, perché in tali situazioni il problema non è meramente tecnico o organizzativo, ma investe direttamente il principio di uguaglianza sostanziale (art. 3 Cost.) e il diritto fondamentale alla tutela

[3] La federazione si basa su un rapporto di fiducia: il servizio riconosce l'autenticazione effettuata da un gestore dell'identità, senza richiedere all'utente credenziali proprie per quel servizio.

della salute (art. 32 Cost.), poiché l'assenza di una classificazione informatica adeguata può tradursi nell'impossibilità concreta di accedere a prestazioni sanitarie cui il paziente avrebbe diritto.

L'identità digitale assume così una funzione giuridica sempre più rilevante, divenendo il presupposto per l'esercizio effettivo di numerosi diritti e servizi pubblici. Proprio per questo la sua disciplina non può essere considerata una questione esclusivamente tecnologica, ma deve essere valutata alla luce dei principi di non discriminazione, proporzionalità ed effettività dei diritti fondamentali sanciti dall'ordinamento europeo.

Più in generale, una democrazia che si fondi esclusivamente su sistemi di identificazione tecnica rischia di perdere il contatto con la persona concreta, sostituendo il cittadino con il profilo e la partecipazione con la verifica. Eppure, anche la democrazia digitale dovrebbe richiedere non solo identità affidabili, ma persone riconosciute come soggetti capaci di azione e di parola, di responsabilità e di relazione **(cfr. Arendt, 1958)**.

Per questo motivo l'infrastruttura dell'identità digitale dovrebbe essere pensata non come il fine, bensì come un mezzo che sia subordinato a una concezione della persona che precede e fonda ogni sistema tecnico.

2.3 Identità digitale, persona e democrazia: il problema del soggetto politico nell'era dell'infosfera

Nella tradizione politica occidentale, l'appartenenza alla comunità dei cittadini e le condizioni della partecipazione hanno assunto forme storicamente diverse. Nella *polis* greca, l'uguaglianza politica riguardava una cerchia limitata di cittadini, con esclusioni incompatibili con l'odierno principio di uguaglianza. La moderna concezione della persona come titolare di diritti non può quindi essere retroproiettata senza distinzioni sul mondo antico. Per la riflessione sull'identità digitale resta centrale il rapporto tra riconoscimento della persona, partecipazione alla vita pubblica e possibilità di attribuire azioni e responsabilità.

Le moderne democrazie costituzionali hanno dato forma a questo nesso riconoscendo la persona quale titolare originaria di diritti, presupposto imprescindibile della cittadinanza democratica come riconosciuto dall'art. 2 della Costituzione italiana, che riconosce e garantisce i diritti inviolabili dell'uomo e richiede al tempo stesso l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale. È proprio in questo principio personalista che si ritrova il fondamento che impedisce di identificare la persona con il solo profilo digitale o con le credenziali tecniche attraverso cui essa viene riconosciuta nei sistemi informatici: la persona precede il dato e non può essere ridotta ad esso.

Questo primato dell'antropocentrismo costituzionale è stato magistralmente codificato da Stefano Rodotà **(2007)**, nel passaggio paradigmatico «dal soggetto alla persona». Secondo il giurista, mentre la categoria astratta di «soggetto» rispondeva alla logica individualistica e proprietaria del mercato, la nozione di «persona» restituisce pienezza al cittadino inserito nelle relazioni sociali e titolare di una dignità originaria. La costituzionalizzazione della persona costituisce pertanto lo scudo formale che impedisce ai moderni sistemi di tracciamento e identificazione tecnica di sovrascrivere l'individualità empirica.

Nel contesto digitale, questi presupposti entrano in crisi.

L'ambiente digitale, per sua natura, è uno spazio di moltiplicazione identitaria. Profili, account, avatar, pseudonimi e identità istituzionali convivono e si sovrappongono, rendendo sempre più difficile stabilire un nesso chiaro tra individuo empirico e identità digitale.

La democrazia digitale non deve essere considerata una semplice estensione tecnologica delle procedure tradizionali (voto online, consultazioni digitali, piattaforme di partecipazione) poiché ciò che è in gioco non è soltanto l'efficienza dei processi decisionali, ma la definizione stessa del soggetto che vi prende parte. Un sistema democratico che identifichi gli individui esclusivamente attraverso attributi tecnici, credenziali numeriche o profili algoritmici rischia di confondere l'identità con la persona, sostituendo la complessità dell'essere umano con un insieme di dati funzionali.

In Vita activa **(Arendt, 1958)**, Hannah Arendt descrive lo *spazio dell'apparire* come lo spazio pubblico che si costituisce quando le persone agiscono e parlano insieme, manifestandosi reciprocamente come eguali e distinte. La riduzione di questo spazio a una dimensione puramente tecnica comporta il rischio di una depoliticizzazione radicale. Nel digitale, tale rischio si manifesta quando la partecipazione è mediata da piattaforme che selezionano, filtrano e gerarchizzano le voci attraverso logiche algoritmiche opache, trasformando il dibattito pubblico in una somma di flussi informativi governati da criteri di visibilità e rendimento.

Jürgen Habermas **(Habermas, 1992)** ha insistito sul fatto che la legittimità democratica derivi da processi comunicativi fondati sulla partecipazione simmetrica e inclusiva. Nello spazio digitale, tuttavia, queste condizioni sono spesso compromesse: l'accesso alle tecnologie non è universalmente garantito, le competenze digitali sono distribuite in modo diseguale e gli algoritmi che regolano la circolazione delle informazioni introducono asimmetrie strutturali che alterano la possibilità di un confronto «razionale». La promessa di una democrazia più inclusiva rischia di rovesciarsi nel suo contrario, producendo nuove forme di esclusione e di disuguaglianza. Tali criticità

assumono rilievo anche alla luce del principio democratico e dell'effettiva possibilità di esercitare i diritti di partecipazione in condizioni di pari opportunità.

È in questo contesto che emerge con forza la distinzione tra identità digitale e persona digitale, espressione con cui qui non si indica una nuova entità, ma la persona stessa, nella sua unità psichica, spirituale e corporea, in quanto presente e agente nell'ambiente digitale. Mentre la prima tende a essere concepita come un insieme di attributi verificabili e interoperabili, la seconda rinvia a una dimensione più integrale e irriducibile, che concerne il riconoscimento dell'individuo come soggetto morale e politico, portatore di diritti e doveri. Sottolineare il primato antropologico del concetto «persona» in questo contesto consente di comprendere come una democrazia autentica non possa fondarsi esclusivamente su sistemi di identificazione, poiché questi, per quanto sofisticati, non tengono in considerazione la particolarità e l'unicità di ogni essere umano, la sua vulnerabilità e fragilità[4].

La riflessione di Michel Foucault **(Foucault, 1975)** ci consente di comprendere un ulteriore aspetto della questione: ogni infrastruttura tecnologica, lungi dall'essere neutrale, incorpora relazioni di potere e produce specifiche forme di soggettivazione. I sistemi di identità digitale, come le piattaforme di partecipazione politica, non si limitano a registrare le azioni dei cittadini, ma contribuiscono a modellarne i comportamenti, orientandone le scelte attraverso meccanismi di sorveglianza, normalizzazione e *nudging*. In questo scenario, l'autonomia politica non viene soppressa in modo diretto, ma progressivamente erosa, trasformandosi in una libertà condizionata.

Luciano Floridi **(Floridi, 2014)** analizza l'impatto delle tecnologie dell'informazione sulle forme di organizzazione politica, di appartenenza e di partecipazione. Questa analisi offre lo spunto per una riflessione critica: quando la persona viene considerata esclusivamente in funzione del ruolo che svolge nelle reti informative, rischiano di essere trascurate la sua dignità e la sua irriducibilità a un insieme di dati. Da una prospettiva personalista, occorre dunque riaffermare, anche sul piano giuridico, che la persona costituisce il fine dell'ordinamento e non può essere ridotta a mero oggetto di trattamento informazionale o di classificazione algoritmica.

Se la democrazia digitale vuole evitare di diventare una mera tecnocrazia partecipativa, deve interrogarsi sui limiti di tale modello e riaffermare la persona come fine, non come mezzo.

[4] Se per esempio ci si rivolge alla riflessione di Emmanuel Levinas **(Levinas 1961)**, che pone al centro una soggettività esposta al Volto dell'Altro, si sottolinea come questo non possa mai essere pensato come autoreferenziale e chiuso in se stesso.

La sfida della democrazia digitale appare inseparabile dalla questione dell'identità personale. Non si tratta semplicemente di garantire sicurezza, efficienza o scalabilità ai sistemi di partecipazione, ma di preservare le condizioni, anche giuridiche, che rendono possibile il riconoscimento reciproco tra cittadini. Una democrazia che non tenga conto della frammentazione identitaria prodotta dal digitale rischia di fondarsi su soggetti indeboliti, incapaci di riconoscersi come parte di un destino comune.

In conclusione, l'integrazione tra identità digitale, persona e democrazia impone un ripensamento delle categorie politiche tradizionali. Se la tecnologia può ampliare gli spazi di espressione, ciò può avvenire solo a condizione che non si sostituisca la persona con il profilo, la responsabilità con l'attributo, il dialogo con l'interazione algoritmica. Per non tradire se stessa, la democrazia digitale deve restare ancorata a una concezione del soggetto come entità narrativa e moralmente responsabile. La resistenza filosofica alla tecnocrazia partecipativa deve trovare nel Diritto il suo braccio secolare: l'identificazione digitale deve essere normata come uno strumento di inclusione e di esercizio della cittadinanza, garantendo che la persona preceda sempre il dato e rimanga il fine ultimo dell'ordinamento.

3. Diritto, responsabilità e governance dell'identità digitale

3.1 Identità digitale e tutela della persona: diritti e responsabilità

Il contesto giuridico in cui si collocano l'intelligenza artificiale e la conseguente riflessione sull'identità digitale è caratterizzato da una tensione costante tra innovazione tecnologica e tutela dei diritti fondamentali.

Il Diritto, tradizionalmente fondato su categorie relativamente stabili, si trova oggi a confrontarsi con fenomeni in rapido mutamento, che mettono in discussione concetti quali la soggettività e la responsabilità.

L'identità digitale rappresenta una delle sfide più rilevanti sotto questo profilo: non si limita a identificare un soggetto all'interno di sistemi informatici, ma diventa progressivamente la modalità attraverso cui la persona viene riconosciuta e valutata. Profili digitali, dati comportamentali e sistemi di reputazione algoritmica incidono sull'accesso a diritti, opportunità e servizi, spesso senza che l'individuo abbia piena consapevolezza dei meccanismi sottostanti. La questione non riguarda pertanto soltanto la corretta identificazione tecnica del soggetto, ma il rischio che la rappresentazione digitale divenga il criterio prevalente attraverso cui la persona viene valutata e riconosciuta nei sistemi sociali, economici e istituzionali.

Il Regolamento Generale sulla Protezione dei Dati (GDPR) ha costituito un tentativo significativo di riaffermare il rispetto fondante della persona nel trattamento dei dati personali, introducendo principi fondamentali come la liceità, la trasparenza, la

limitazione delle finalità e la minimizzazione dei dati. In particolare, ha cercato di contrastare il rischio di un'oggettivazione dell'individuo, riconoscendo diritti quali l'accesso ai dati, la rettifica e, in alcuni casi, l'oblio.

L'emergere di sistemi basati sull'apprendimento automatico e sulle decisioni automatizzate mette tuttavia in difficoltà l'efficacia di tali strumenti giuridici: la complessità degli algoritmi e la cosiddetta *black box*[5] rendono spesso difficile, se non impossibile, comprendere le ragioni che conducono a una determinata decisione. Ciò solleva interrogativi rilevanti sul significato stesso di trasparenza e sulla possibilità di un consenso realmente informato e una partecipazione attiva della persona alla gestione e all'utilizzo dei dati che la rappresentano. La trasparenza non può, infatti, essere intesa come semplice disponibilità di informazioni tecniche sul funzionamento del sistema, ma deve tradursi nella possibilità concreta per la persona interessata di comprendere, contestare e, ove necessario, ottenere una revisione della decisione che la riguarda. In questa direzione si muovono l'art. 22 del GDPR, che riconosce il diritto di non essere sottoposti, salvo le eccezioni previste, a decisioni basate unicamente su un trattamento automatizzato che producano effetti giuridici o incidano in modo analogo significativamente sulla persona, e l'art. 86 dell'*AI Act*, che riconosce il diritto di ottenere spiegazioni chiare e significative sul ruolo svolto da determinati sistemi ad alto rischio nelle decisioni che la riguardano.

Un ulteriore nodo critico riguarda la responsabilità giuridica. Quando una decisione viene presa o fortemente influenzata da un sistema di intelligenza artificiale, diventa complesso individuare il soggetto responsabile: il programmatore, il fornitore del sistema, l'ente che lo utilizza o l'operatore umano che si limita a recepirne l'esito? Va però precisato che l'introduzione di sistemi di AI nei processi decisionali non determina un trasferimento della responsabilità dalla persona alla macchina; rimane necessario individuare i soggetti responsabili secondo una logica di *accountability*, evitando che l'opacità tecnologica produca una zona di deresponsabilizzazione incompatibile con i principi dello Stato di diritto.

L'*AI Act* dell'Unione europea (Regolamento (UE) 2024/1689) adotta un approccio basato sul rischio per tutelare la salute, la sicurezza e i diritti fondamentali. Prevede obblighi specifici per i sistemi classificati ad alto rischio in base alle loro finalità e alle condizioni stabilite dal regolamento. Vi rientrano, alle condizioni previste, determinati sistemi impiegati nei dispositivi medici, nell'amministrazione della giustizia e nell'identificazione

[5] Il termine *black box* indica un sistema di cui si conoscono l'input (i dati in entrata) e l'output (i risultati in uscita), ma di cui sono ignoti o inaccessibili i processi interni. Nei modelli di intelligenza artificiale, l'utente non può vedere il percorso logico seguito per generare un risultato.

biometrica remota. Per alcune pratiche considerate incompatibili con la tutela dei diritti fondamentali, il regolamento stabilisce invece divieti.

Nonostante l'importanza di questo tentativo normativo, resta aperta la questione della reale capacità del Diritto di governare tecnologie che evolvono più rapidamente delle leggi. Il rischio è che la regolamentazione intervenga sempre in ritardo, limitandosi a inseguire l'innovazione anziché orientarla secondo valori condivisi.

Da qui la necessità di affiancare alla dimensione giuridica una riflessione etica e culturale più ampia. Il Diritto non può garantire la tutela della persona se non è sostenuto anche da una consapevolezza diffusa e da una responsabilità condivisa nell'uso delle tecnologie. L'identità digitale e l'AI pongono, dunque, una sfida che è insieme normativa e profondamente antropologica.

Accanto alla riservatezza e alla protezione dei dati, l'ordinamento conosce un diritto all'identità personale: il diritto a non vedere travisata la rappresentazione pubblica di sé. Ricondotto dalla giurisprudenza all'art. 2 della Costituzione, esso vale qui soprattutto come indizio: il diritto riconosce, e non istituisce, che la persona non coincide con le immagini che di lei circolano. La sua tutela presuppone però che il travisamento sia riconducibile a qualcuno. Nella frammentazione digitale (§ 1.5), invece, non c'è un singolo atto né un singolo responsabile: la distorsione nasce dall'insieme dei profili, anche quando ciascuno di essi, preso da solo, è corretto. Il travisamento, prima di essere un illecito, è un mancato riconoscimento: la tutela giuridica è necessaria, ma la questione resta antropologica ed etica.

Per l'ampia platea di utenti non specialisti che utilizza quotidianamente la rete, è fondamentale comprendere che tutelare le informazioni personali significa proteggere anche la propria autonomia e identità. Nella prospettiva di Floridi **(Floridi, 2014)**, la *privacy* assume un valore costitutivo, perché riguarda la possibilità di formare e preservare la propria identità personale. La protezione dei dati contribuisce a contrastare ingerenze indebite, manipolazioni e condizionamenti, senza eliminare ogni influenza esterna. Le ricerche *online*, le pagine visitate, gli acquisti e le conversazioni possono rivelare aspetti significativi dei nostri bisogni, delle nostre convinzioni e intenzioni. Le tracce digitali consentono così di costruire profili capaci di incidere sulla rappresentazione sociale della persona e sulle opportunità che le vengono offerte, pur restando rappresentazioni parziali, che non ne esauriscono l'identità.

Come già osservato (§ 1.2), il rischio di riduzionismo emerge quando la persona viene identificata esclusivamente con profili e correlazioni statistiche ricavati dai suoi dati. In questa prospettiva, dimensioni fondamentali dell'esperienza umana, quali corporeità, libertà, creatività e imprevedibilità, rischiano di essere trascurate perché non pienamente rappresentabili dai modelli utilizzati. Una scarsa consapevolezza di questi processi può rendere più difficile riconoscere e valutare i danni che la raccolta e l'uso

delle tracce digitali possono produrre nel presente e nel futuro. I dati, una volta condivisi in rete, possono sfuggire in parte al nostro controllo effettivo e risultare difficili da recuperare o cancellare integralmente. Pur restando esercitabili i diritti riconosciuti dalla normativa sulla protezione dei dati personali, sul piano concreto può accadere che la persona perda la capacità di governarne pienamente la circolazione e l'utilizzo: di fatto, è come se quei dati non le appartenessero più. Se perdiamo la capacità di controllo su ciò che esprimiamo in rete, emerge la necessità di rafforzare i diritti con cui mantenere una sovranità su ciò che è nostro anche nello spazio digitale, e ancor più quella di uno sguardo critico verso le nuove tecnologie.

Inoltre, l'ambiente digitale rischia di creare nuove forme di discriminazione (si pensi, ad esempio, alle limitazioni anagrafiche, come accade agli anziani, alle restrizioni economiche, come ai più poveri, alle barriere culturali) che determinano l'impossibilità di accedere ad alcuni servizi e l'incapacità di esercitare diritti fondamentali all'informazione, alla salute, alla cultura. Il profilo di criticità sta nel rischio che l'identità digitale, anziché favorire l'inclusione, produca nuove forme di esclusione sociale e giuridica. L'accesso ai servizi digitali presuppone infatti non soltanto la disponibilità di infrastrutture tecnologiche, ma anche adeguate competenze digitali e condizioni materiali di accesso. La cosiddetta alfabetizzazione digitale diventa così un elemento determinante per l'effettiva fruizione dei diritti, con il rischio che persone prive degli strumenti necessari restino escluse, con forme di esclusione spesso non immediatamente visibili, perché non derivano da divieti espliciti, ma dall'organizzazione stessa dei sistemi digitali e dai requisiti necessari per potervi e sapervi accedere. In questa prospettiva, il principio di uguaglianza reale, previsto costituzionalmente, richiede che la trasformazione digitale non si limiti a garantire efficienza e interoperabilità ma assicuri condizioni reali di accessibilità e inclusione per tutti i cittadini.

3.2 Regolamentazione e governance

3.2.1 La necessità di una governance dell'innovazione

L'attuale trasformazione tecnologica rende evidente la necessità di una *governance* dell'innovazione. La questione riguarda direttamente l'identità digitale: i sistemi di intelligenza artificiale operano sui profili, sulle inferenze e sulle classificazioni attraverso cui la persona viene rappresentata, e governarli significa anche stabilire come, da chi e con quali limiti essa possa essere definita. L'AI non può essere lasciata esclusivamente alle dinamiche del mercato o all'iniziativa privata, poiché le sue applicazioni incidono direttamente sui diritti fondamentali, sulla sicurezza e sul benessere delle persone.

Governare i nuovi sistemi digitali significa definire regole, limiti e responsabilità, ma anche orientare lo sviluppo tecnologico secondo valori condivisi. In assenza di una *governance* efficace, il rischio è quello di una frammentazione normativa e di un utilizzo

disomogeneo delle tecnologie, con conseguenze potenzialmente dannose per la tutela dei diritti.

In ambito sanitario, la crescente integrazione delle tecnologie digitali rende necessario un modello di *governance* capace di coniugare innovazione tecnologica e tutela dei diritti fondamentali. La questione non riguarda infatti soltanto la possibilità tecnica di raccogliere, elaborare e utilizzare grandi quantità di dati, ma le condizioni stesse entro cui tale utilizzo possa ritenersi compatibile con la dignità della persona, la sua autonomia e il principio di equità.

Tale modo di governare il sistema, però, non può ridursi a un insieme di norme tecniche: deve includere dimensioni etiche, sociali e culturali. Solo un approccio integrato può consentire di affrontare la complessità delle trasformazioni in atto e di evitare che l'innovazione tecnologica si sviluppi secondo logiche esclusivamente tecniche o di mercato, prive di un adeguato presidio etico e giuridico.

La mercificazione algoritmica del profilo umano trova un limite concettuale fondamentale nella riflessione di Luca Bolognini **(Bolognini, 2021)** in merito alla convergenza tra le regolazioni dei mercati *data-driven* e la tutela dei diritti fondamentali. Nella presentazione del volume il monito biblico viene parafrasato in un'efficace chiave contemporanea: «*memento homo quia data es et in data reverteris*». La datificazione totale dell'universo sociale ed economico impone una *governance* che non sia mera compliance burocratica, bensì un argine etico-giuridico a presidio del Sé contro le spinte estrattive delle piattaforme digitali.

3.2.2 Le sfide del Diritto nel controllo dell'innovazione tecnologica

Le istituzioni pubbliche devono avere chiaro il proprio ruolo centrale nella regolamentazione dell'intelligenza artificiale: il Diritto rappresenta uno strumento fondamentale per garantire che lo sviluppo tecnologico avvenga nel rispetto dei principi democratici e dei diritti fondamentali, non limitandosi a disciplinare gli effetti già prodotti dall'innovazione, ma orientando preventivamente i processi tecnologici verso modelli compatibili con la tutela della persona. Se di fatto, come si è visto (§ 3.1), la regolamentazione tende spesso a intervenire in ritardo, l'obiettivo resta quello di un Diritto capace di orientare, e non soltanto di inseguire, l'innovazione.

Il GDPR e l'*AI Act*, già illustrati al § 3.1, costituiscono riferimenti essenziali di questo percorso. La sfida consiste nel tradurne le garanzie in criteri effettivi di progettazione, impiego e controllo delle tecnologie.

In una lettura personalista, il dato deve essere considerato nel suo legame con la persona cui si riferisce e con gli effetti che il suo utilizzo può produrre sulla sua vita. In ambito sanitario ciò assume un valore particolare: il dato relativo alla salute non costituisce una semplice informazione tecnica, ma riguarda la storia personale e le

vulnerabilità della persona assistita. La sua protezione deve quindi accompagnare l'intero percorso di innovazione.

Governare questo percorso richiede modelli capaci di anticipare i rischi, verificare gli effetti concreti delle applicazioni e adeguare le garanzie al mutare dei contesti. Il compito del Diritto è accompagnare l'innovazione, mantenendola subordinata alla tutela della persona e dei suoi diritti fondamentali.

3.3 Modelli di governance etica per un uso responsabile: trasparenza, controllo e responsabilità

La tecnologia può essere realmente al servizio della cura e della società solo se rimane collocata entro un preciso orizzonte di responsabilità: la tecnologia come strumento, la persona come fine e la responsabilità come principio che non può essere integralmente delegato ai sistemi automatizzati.

La cornice di garanzia e di tutela dei diritti fondamentali offerta dal Diritto non può tuttavia sostituire una *governance* responsabile che non deve inseguire la tecnologia, ma governarla senza pretendere di eliminarne la complessità.

Uno dei pilastri della *governance* dei nuovi sistemi digitali è la *trasparenza*: assicurare un livello adeguato di spiegabilità dei sistemi di AI, almeno nei loro principi fondamentali, è una condizione essenziale per garantire il controllo umano e la possibilità di contestare le decisioni automatizzate. Per i sistemi di identità digitale, ciò significa poter conoscere quali dati e quali inferenze concorrono a definire il proprio profilo e da chi vengono utilizzati.

La trasparenza è strettamente legata alla responsabilità: senza una chiara attribuzione di quest'ultima, diventa difficile tutelare i diritti delle persone e garantire rimedi efficaci in caso di danni. La *governance* dell'AI deve quindi prevedere meccanismi di tracciabilità delle decisioni e di *accountability* degli attori coinvolti perché la responsabilità non riguarda esclusivamente il momento patologico dell'eventuale danno, ma costituisce un criterio ordinario di progettazione, implementazione e impiego dei sistemi di intelligenza artificiale, secondo un approccio preventivo ormai proprio della regolamentazione europea.

In questo contesto, assume particolare rilievo il ruolo delle competenze interdisciplinari; giuristi, tecnologi, eticisti e professionisti dei settori di applicazione devono collaborare per progettare sistemi digitali che siano non solo efficienti, ma anche giusti e affidabili.

La *governance* dell'AI non può, però, essere ad appannaggio esclusivo di esperti e istituzioni. È necessario promuovere una diffusa cultura della cittadinanza digitale che consenta ai cittadini di comprendere le implicazioni dei sistemi di intelligenza artificiale

e di partecipare attivamente al dibattito pubblico. Sul ruolo della formazione e dell'educazione digitale si tornerà più avanti (§§ 5.4.2 e 6.4). È in questa prospettiva che la *governance* dell'AI può diventare un processo condiviso che coinvolga Istituzioni, comunità scientifica e società civile: solo attraverso un dialogo aperto e informato sarà possibile costruire un quadro regolatorio capace di coniugare innovazione e tutela della persona.

4. Identità digitale nella società algoritmica: decisioni automatizzate, servizi e sanità

4.1 Dalla società industriale alla società algoritmica

Per comprendere le implicazioni di un'identità personale sempre più mediata attraverso la dimensione digitale, è necessario tornare su alcune questioni centrali della rivoluzione digitale, in particolare sul passaggio epocale dalla società industriale a quella algoritmica. Senza chiarire le dinamiche di controllo, decisione e responsabilità che caratterizzano quest'ultima, non è possibile cogliere appieno le implicazioni di tale trasformazione.

Nella società industriale la tecnica trasformava soprattutto la materia e il lavoro: la macchina sostituiva o potenziava la forza fisica, mentre le decisioni sulle persone restavano affidate a istituzioni e a soggetti riconoscibili. Nella società algoritmica la tecnica opera invece sull'informazione e, attraverso di essa, sulle persone stesse: classifica, prevede, attribuisce punteggi. È qui che la questione tecnologica diventa questione di identità, perché il modo in cui un sistema rappresenta una persona finisce per incidere su ciò che le è concesso o negato.

La cultura algoritmica contemporanea non solo supporta attività operative, ma assume un ruolo sempre più centrale nei processi decisionali: ordinando e classificando idee, oggetti e persone, orienta scelte economiche, politiche e sociali, influenzando l'allocazione delle risorse, la definizione delle priorità e la gestione dei rischi. In tale prospettiva gli algoritmi non si limitano a descrivere la realtà, ma contribuiscono progressivamente a organizzarla e a condizionarla, incidendo sulle modalità attraverso cui vengono riconosciuti bisogni, opportunità e priorità.

La progressiva integrazione degli algoritmi nei processi decisionali pone, pertanto, una questione non solo tecnologica ma anche giuridica, poiché l'esercizio del potere decisionale incide direttamente sulla tutela dei diritti fondamentali e sull'attribuzione delle responsabilità.

La società algoritmica si caratterizza per una crescente automatizzazione delle decisioni, che tende a ricondurre la complessità del reale a modelli calcolabili. Questo processo, se da un lato consente una gestione più efficiente dei sistemi complessi,

dall'altro rischia di semplificare eccessivamente fenomeni che richiederebbero una valutazione qualitativa e contestuale, propria del giudizio umano.

4.2 Il potere predittivo degli algoritmi, automazione e controllo

4.2.1 Il potere predittivo degli algoritmi e il rischio di determinismo

Uno degli aspetti più significativi e, al tempo stesso, più problematici della rivoluzione digitale è l'affermarsi del potere predittivo dell'AI. Attraverso l'analisi dei dati, gli algoritmi sono in grado di anticipare comportamenti, individuare tendenze e suggerire azioni future. Questo potere predittivo trova applicazione in numerosi ambiti: dalla sicurezza alla sanità, dal marketing alla gestione delle risorse umane. Tuttavia, la capacità di previsione degli algoritmi può generare forme di *determinismo* tecnologico: quando una previsione viene assunta come certezza, essa rischia di trasformarsi in una profezia che si autoavvera. La conseguenza ad alto rischio è che le persone vengano trattate in base a ciò che gli algoritmi prevedono che faranno, riducendo lo spazio per il cambiamento e la libertà individuale. Sul piano dell'identità, ciò significa che il profilo predittivo tende a fissare la persona in ciò che è stata, sottraendole la libertà di cambiare e di crescere. Tale rischio è particolarmente evidente nei contesti in cui le decisioni automatizzate hanno un impatto diretto sulla vita delle persone, come ad esempio nella valutazione del rischio, nella concessione di benefici o nella selezione lavorativa, dove il potere predittivo degli algoritmi può rafforzare disuguaglianze preesistenti e cristallizzare situazioni di svantaggio. In tali contesti il rischio non è soltanto tecnico, ma giuridico: decisioni fondate prevalentemente su valutazioni predittive possono incidere sui principi di uguaglianza, non discriminazione e proporzionalità, imponendo che il ricorso agli strumenti algoritmici sia sempre accompagnato da adeguate garanzie procedurali e da un controllo umano effettivo.

4.2.2 Automazione, decisione e responsabilità

La crescente automazione dei processi decisionali solleva interrogativi profondi sulla responsabilità umana. Quando una decisione viene presa o suggerita da un sistema artificiale, si tende a considerarla più oggettiva – anche se solo apparentemente tale – e affidabile, riducendo la propensione a metterla in discussione; il mondo sanitario non è estraneo a queste dinamiche, anche per il timore delle conseguenze medico-legali che ne possano derivare.

Questo fenomeno può condurre a una progressiva perdita di responsabilità, nel momento in cui gli esseri umani finiscono per limitarsi a eseguire o ratificare decisioni algoritmiche senza esercitare un reale controllo critico. La delega alla macchina diventa così una forma di deresponsabilizzazione che indebolisce la capacità di giudizio individuale e collettivo, ponendo la questione dell'imputazione della responsabilità non solo sul piano giuridico, ma anche su quello etico. Assumere una decisione significa, infatti, rispondere delle conseguenze e accettarne il peso morale: quando la decisione

viene attribuita a un algoritmo, questo legame tra scelta e responsabilità rischia di spezzarsi.

Recuperare uno spazio di responsabilità umana all'interno dei sistemi automatizzati rappresenta una delle sfide centrali della società contemporanea e ciò richiede non soltanto strumenti normativi adeguati coerenti con il principio della supervisione umana significativa (*meaningful human oversight*), ma anche una cultura della consapevolezza e del limite.

4.2.3 La questione del controllo umano sulle decisioni e la dipendenza dagli algoritmi

All'interno della trasformazione sociale indotta dalla rivoluzione digitale emerge una questione centrale: fino a che punto il governo delle decisioni rimane effettivamente umano? I sistemi algoritmici non si limitano a fornire strumenti di supporto, ma contribuiscono a strutturare il campo delle possibilità, orientando scelte individuali e collettive.

La loro forza risiede nella capacità di analizzare grandi quantità di dati e di produrre valutazioni predittive. Proprio questa capacità, però, può generare la forma di dipendenza già descritta (§ 4.2.2): il pericolo non è tanto la sostituzione dell'uomo, quanto una progressiva delega decisionale che riduce attenzione critica e responsabilità personale.

In ambiti particolarmente sensibili, come ad esempio l'accesso ai servizi, il credito, la giustizia o la sanità, questo può trasformare il ruolo dei professionisti e incidere sull'autonomia dei soggetti coinvolti. L'operatore rischia di diventare esecutore di indicazioni generate da sistemi opachi, mentre la persona destinataria della decisione fatica a comprendere o contestare il processo che l'ha determinata.

Il controllo umano non può essere inteso come semplice supervisione formale: richiede trasparenza, comprensibilità e reale possibilità di intervento. Solo in questo modo i sistemi di intelligenza artificiale possono rimanere strumenti al servizio della persona. Il controllo umano, infatti, non costituisce un ostacolo all'innovazione, ma la condizione affinché le decisioni algoritmiche restino sottoposte alla responsabilità di chi le adotta e siano sempre contestabili, verificabili e orientate alla tutela dei diritti fondamentali. È nella relazione di cura, dove la persona si presenta nella condizione di maggiore vulnerabilità, che queste dinamiche mostrano le conseguenze più delicate.

4.3 L'impatto delle tecnologie sui servizi e sulla cura

L'innovazione tecnologica non produce soltanto nuovi strumenti, ma modifica concretamente le modalità attraverso cui le istituzioni, i professionisti e i cittadini accedono ai servizi e vivono l'esperienza della cura. Per questo motivo, la valutazione delle tecnologie digitali non può limitarsi ai criteri di efficienza o di prestazione, ma deve

interrogarsi sulla loro capacità di promuovere relazioni di cura rispettose della dignità, dell'autonomia e delle vulnerabilità della persona.

4.3.1 Innovazione tecnologica e miglioramento dei servizi

Pur con le criticità evidenziate nei capitoli precedenti, l'identità digitale intesa come insieme strutturato di dati, informazioni e profili che rappresentano la persona nei contesti digitali può offrire contributi significativi al miglioramento dei servizi pubblici e privati. Quando è inserita entro un adeguato quadro di garanzie giuridiche ed etiche, essa consente una gestione più efficace delle informazioni, favorendo processi decisionali più tempestivi e mirati.

L'intelligenza artificiale rappresenta uno dei principali motori dell'innovazione tecnologica contemporanea. La sua capacità di analizzare grandi quantità di dati e di individuare schemi complessi consente di migliorare l'efficienza e la qualità di numerosi servizi (pubblici e privati), ottimizzare i processi, ridurre i tempi di risposta e aumentare la precisione delle attività svolte. Non bisogna tuttavia sottovalutarne gli aspetti critici.

Nel contesto dei servizi pubblici, l'intelligenza artificiale può contribuire a una gestione più efficace delle risorse, favorendo una distribuzione più equa e mirata degli interventi; i sistemi di supporto decisionale possono aiutare le amministrazioni a individuare bisogni emergenti, prevenire situazioni di criticità e migliorare la pianificazione delle politiche pubbliche. Affinché tali strumenti siano realmente orientati al bene comune, è tuttavia necessario che il loro impiego avvenga nel rispetto dei principi di trasparenza, proporzionalità, non discriminazione ed equità che caratterizzano l'azione amministrativa e la tutela dei diritti.

Se correttamente utilizzati, questi sviluppi offrono l'opportunità di rendere i servizi più accessibili e personalizzati, rispondendo in modo più adeguato alle esigenze dei cittadini. La sfida consiste nell'evitare che l'innovazione tecnologica si traduca in una semplificazione eccessiva dei problemi o in una riduzione della complessità sociale a meri indicatori quantitativi.

La condizione essenziale, in ogni caso, è che l'identità digitale rimanga uno strumento al servizio della persona e non un criterio esclusivo di valutazione.

4.3.2 Efficienza, prevenzione e qualità della vita

Uno dei contributi potenziali della rivoluzione digitale riguarda la prevenzione. L'analisi predittiva può aiutare a individuare condizioni di rischio e a orientare interventi tempestivi, anche prima della manifestazione di una patologia. L'effettivo miglioramento degli esiti di salute e l'eventuale riduzione dei costi devono tuttavia essere verificati nei singoli contesti, considerando l'affidabilità dei modelli, la qualità dei dati e l'integrazione degli strumenti nei percorsi assistenziali.

I cambiamenti tecnologici trovano applicazione nel miglioramento della qualità della vita delle persone più fragili. Le tecnologie robotiche e i sistemi di intelligenza artificiale possono supportare l'autonomia di anziani e delle persone con disabilità, facilitando la gestione delle attività quotidiane e migliorando la sicurezza.

Questi benefici, tuttavia, non devono far perdere di vista la necessità di una supervisione umana effettiva. Efficienza e prevenzione non possono diventare criteri assoluti, pena il rischio di sacrificare la dimensione umana e relazionale sull'altare dell'ottimizzazione.

4.3.3 Il ruolo della tecnologia nelle relazioni

Un elemento chiave nella valutazione degli impatti positivi della rivoluzione digitale riguarda il suo ruolo di supporto all'agire umano. Quando l'essere umano è affiancato nelle attività complesse da strumenti sofisticati di analisi e di previsione, ne trae sicuramente un beneficio, purché ciò non comporti una sostituzione del giudizio umano. Ciò vale soprattutto nei contesti che coinvolgono diritti fondamentali e decisioni eticamente sensibili, i quali richiedono sempre una valutazione contestuale e un'assunzione di responsabilità non delegabile ai sistemi automatizzati.

Nel settore sanitario, le nuove tecnologie possono rappresentare un valido alleato del medico, ma non possono sostituire la relazione terapeutica, l'ascolto e la capacità di interpretare il vissuto del paziente. Il rischio di una delega totale alla tecnologia è quello di trasformare la cura in un processo impersonale in cui il paziente diventa un insieme di dati da elaborare.

La centralità della persona nella cura può essere approfondita mettendo in dialogo la bioetica personalista con le riflessioni di Paul Ricœur ed Emmanuel Levinas, pur nella diversità delle rispettive prospettive. Ricœur riconosce nel patto di cura fondato sulla fiducia il nucleo etico della relazione tra medico e paziente **(Ricœur, 1996)**; Levinas mostra come l'incontro con il volto dell'altro chiami alla responsabilità **(Levinas, 1961)**. Questi contributi aiutano a riconoscere nel malato una persona nella sua singolarità e vulnerabilità, la cui esperienza eccede i parametri clinici che la descrivono. Le tecnologie possono sostenere la relazione di cura, ma non esaurirne la dimensione umana e morale.

Riconoscere il valore del supporto (anziché della sostituzione) significa adottare un approccio prudente, garantendo che il digitale rimanga uno strumento al servizio della cura e mai un criterio di riduzione dell'umano.

Le potenzialità dell'identità digitale nei servizi e nella cura mostrano, dunque, come l'innovazione tecnologica possa effettivamente contribuire al miglioramento della qualità della vita. Proprio nei contesti in cui essa si rivela più promettente, però,

emergono con maggiore evidenza le questioni etiche, giuridiche e antropologiche che ne accompagnano l'utilizzo.

4.4 L'identità digitale in ambito sanitario

Il settore sanitario rappresenta uno degli ambiti in cui le nuove tecnologie mostrano le potenzialità più rilevanti. La raccolta e l'organizzazione dei dati clinici consentono una visione più integrata del percorso di cura del paziente, facilitando la continuità assistenziale e la condivisione delle informazioni tra professionisti. Tale continuità assistenziale, tuttavia, richiede che la circolazione delle informazioni avvenga nel rispetto dei principi di riservatezza, sicurezza e proporzionalità, affinché la condivisione del dato sanitario rimanga funzionale alla cura e non si traduca in un'indebita compressione della sfera personale del paziente.

Sistemi di intelligenza artificiale sono già impiegati nel supporto alla diagnosi, nell'analisi delle immagini mediche, nella gestione dei dati clinici e nella stima dell'evoluzione di determinate patologie. In applicazioni specifiche possono migliorare l'accuratezza diagnostica e favorire l'individuazione precoce di condizioni di rischio; tali benefici richiedono però una validazione clinica adeguata e una verifica delle prestazioni nelle popolazioni e nei contesti in cui i sistemi vengono utilizzati.

L'analisi strutturata dei dati sanitari può favorire diagnosi più tempestive, una migliore individuazione dei fattori di rischio e una maggiore personalizzazione dei trattamenti. In questo senso, l'identità digitale diventa uno strumento che può sostenere una medicina più precisa e attenta alle caratteristiche individuali.

Il dato sanitario, tuttavia, non rappresenta soltanto un'informazione clinica utile ai fini diagnostici o organizzativi: esso custodisce la storia della persona, rinvia alla sua fragilità costitutiva e al rapporto di fiducia che si instaura con i professionisti della cura. Per questo motivo il suo trattamento richiede non solo adeguate misure di sicurezza, ma anche un costante orientamento al rispetto della dignità e dei diritti della persona assistita.

Dal punto di vista organizzativo, l'integrazione dei dati consente una gestione più efficiente delle strutture sanitarie, ottimizzando risorse e tempi. Tuttavia, anche in questo contesto, l'efficienza non può sostituire la relazione di cura, che resta il cuore dell'esperienza sanitaria. Il processo decisionale clinico continua infatti a richiedere il giudizio del professionista, il dialogo con il paziente e l'assunzione della responsabilità terapeutica, elementi che nessun sistema algoritmico può sostituire.

Laddove l'identità digitale diventa il principale strumento attraverso cui la persona viene rappresentata, valutata e assistita, occorre interrogarsi sui limiti, sulle garanzie, sulle responsabilità e sui criteri che ne devono orientare l'impiego. Efficienza,

personalizzazione e prevenzione non possono trasformarsi in parametri esclusivi, pena il rischio di ridurre la persona a un insieme di dati.

È dunque necessario passare da una riflessione sulle opportunità a un'analisi più approfondita delle implicazioni etiche, giuridiche e sociali, affinché l'uso dell'identità digitale resti coerente con il rispetto della dignità della persona, della sua autonomia e del valore insostituibile della relazione di cura.

5. Cura, dignità ed etica della progettazione: custodire l'umano

5.1 Custodire l'umano e le nuove sfide etiche

Se mai vi fu un tempo in cui l'uomo dovette interrogare con maggiore urgenza se stesso circa il senso del proprio agire tecnico, quel tempo è il nostro. Poiché le macchine, nate come strumenti docili al servizio della mano umana, hanno ormai assunto il ruolo di mediatrici dell'identità, del riconoscimento, della cura e perfino della dignità, diviene necessario non soltanto regolarne l'uso, ma comprenderne l'impatto sull'essere umano nella sua interezza corporea, relazionale e morale. Non è in gioco un semplice progresso funzionale, bensì la forma stessa della vita comune. Le tecnologie digitali, e in particolare i sistemi di identità, non sono strumenti neutrali: plasmano relazioni sociali, distribuiscono potere e condizionano l'accesso a diritti e opportunità. L'identità digitale è ormai un ambito in cui scelte tecniche e scelte etiche coincidono, poiché assegnare identità significa esercitare potere. Per questo motivo, la progettazione delle infrastrutture digitali non può essere considerata un'attività esclusivamente tecnica, ma assume una rilevanza costituzionale e giuridica, incidendo concretamente sull'effettività dei diritti fondamentali e sul principio di uguaglianza.

Se la riflessione etica deve assumere un ruolo centrale, occorre anzitutto rilevare come oggi tutto sembri essere «etica»: etica dell'AI, etica dei dati, etica della sorveglianza. Eppure, proprio mentre l'etica viene proclamata ovunque, essa rischia di svuotarsi, ridotta a un prontuario di soluzioni rapide, a un elenco di principi da applicare come un cerotto su ferite che non si vogliono guardare. Parlare di etica non significa avere risposte: significa saper porre le domande giuste, domande che non chiudono il discorso, ma lo aprono; domande che non rassicurano, ma inquietano; non quelle che cercano l'efficienza, ma quelle che cercano la verità dell'esperienza umana.

In questo quadro, l'etica non può essere un'aggiunta tardiva, ma deve costituire una dimensione strutturale della progettazione. Etica della cura, dignità della persona e identità digitale vanno perciò pensate insieme, in un'unica architettura teorica, per mostrare come le nuove tecnologie non siano un ambito neutrale di applicazione tecnica, ma un luogo eminentemente morale in cui si decide se l'umano venga custodito o dissolto. Custodire l'umano **(Leone XIV, 2026)** significa allora progettare tecnologie che riconoscano la persona non come semplice destinataria di servizi, ma come

soggetto di diritti, portatrice di una fragilità costitutiva che il Diritto è chiamato a proteggere e che la tecnica è chiamata a rispettare.

5.2 La crisi dell'etica nell'era digitale

Il rischio di svuotamento appena richiamato ha una radice precisa: l'etica digitale contemporanea, pur proliferando in codici, linee guida e dichiarazioni di principio, appare spesso priva di un fondamento filosofico unitario e si riduce facilmente a una logica di mera conformità normativa, incapace di interrogare le premesse antropologiche implicite nei sistemi tecnologici. Una prospettiva personalista, che radica la dignità nell'essere stesso della persona, offre invece un criterio di giudizio e non un semplice elenco di principi.

Quando si invoca il «primato antropologico dell'essere umano», raramente si chiarisce quale concezione di umano venga presupposta. Il soggetto astratto, razionale e autosufficiente ereditato dalla modernità giuridica si rivela inadeguato a descrivere l'essere umano concreto: incarnato, costituzionalmente fragile e quindi dipendente da relazioni di cura e riconoscimento. È invece questa concezione della persona concreta, e non quella del soggetto astratto, a ispirare il costituzionalismo contemporaneo e il sistema europeo dei diritti fondamentali, nei quali dignità, uguaglianza e autonomia costituiscono il parametro entro cui valutare anche la legittimità delle innovazioni tecnologiche.

La rivoluzione digitale, nel momento stesso in cui promette efficienza e ottimizzazione, mette a nudo questa inadeguatezza. Esistono, del resto, casi concreti che mostrano come scelte tecniche apparentemente neutre abbiano conseguenze morali: i sistemi di autenticazione che escludono persone con disabilità; i servizi digitali che penalizzano chi non possiede uno smartphone; i sistemi nazionali che non contemplano identità minoritarie. Questi esempi mostrano che l'identità digitale è un luogo di tensione tra inclusione ed esclusione, tra riconoscimento e invisibilità.

Le attuali tecnologie biometriche costituiscono il luogo paradigmatico di tale tensione. Esse operano una traslazione silenziosa ma radicale: il corpo, da luogo vissuto dell'esperienza, diviene superficie di estrazione informazionale. Caratteristiche del volto, dell'iride, delle impronte e del comportamento possono essere elaborate per riconoscere o verificare l'identità di una persona. Quando i dati biometrici sono trattati per identificare in modo univoco una persona fisica, il GDPR li sottopone al regime previsto per le categorie particolari di dati personali, vietandone in linea generale il trattamento, salvo i casi e le condizioni previsti dalla normativa[6]. Si tratta di una tutela che opera già a monte, indipendentemente dal fatto che il trattamento conduca o meno a una decisione automatizzata.

Eppure, il corpo non è un oggetto tra gli oggetti: è il modo originario con cui l'essere umano è al mondo. Ridurlo a identificatore significa smarrire la distinzione fondamentale tra persona e cosa. Quando il riconoscimento fallisce, quando l'algoritmo non vede, non riconosce, non ammette, non si produce semplicemente un errore tecnico, ma una ferita etica e giuridica: l'individuo viene sospeso nella propria esistenza sociale. È proprio in questo spazio, in cui il riconoscimento tecnico rischia di sostituire il riconoscimento della persona, che emerge una delle questioni etiche più profonde della trasformazione digitale: come custodire un'identità che non sia soltanto verificata dai sistemi, ma autenticamente riconosciuta nella sua dignità, nella sua fragilità costitutiva e nei diritti che da essa derivano.

5.3 Etica della progettazione e dignità della persona

5.3.1 Identità digitale e potere di definizione

L'identità digitale non è una mera estensione funzionale dell'identità civile: è un dispositivo di potere, poiché, come si è visto a proposito dei quadri di fiducia (§ 2.1.1), stabilisce chi può essere riconosciuto, a quali condizioni e secondo quali categorie. Ogni sistema identitario seleziona, semplifica, normalizza. Qui emerge con chiarezza il carattere etico della progettazione: decidere quali attributi contino, quali eccezioni siano ammesse e quali forme di opacità siano tollerate equivale a decidere quali vite siano pienamente intelligibili e quali restino ai margini. I casi di esclusione sistematica (dalle persone con disabilità alle minoranze etniche e sociali) mostrano che l'identità digitale può trasformarsi da strumento di inclusione a meccanismo di «invisibilizzazione».

5.3.2 La dignità come fondamento non negoziabile

Contro ogni riduzionismo funzionalista, l'approccio dignitario riafferma che l'essere umano possiede un valore intrinseco che non dipende da prestazioni, utilità o

[6] Cfr. Regolamento (UE) 2016/679, art. 9, paragrafi 1 e 2, sul trattamento delle categorie particolari di dati personali.

conformità a modelli normativi. La dignità è un concetto pre-giuridico, non è un premio né un risultato: è una condizione originaria. Ne discende un principio decisivo: nessun sistema tecnologico può essere moralmente giustificato se tratta l'essere umano come mero mezzo, come risorsa informazionale o come oggetto di ottimizzazione. La persona non è un automa naturale né una macchina imperfetta; è un essere umano dotato di coscienza, capace di soffrire, di narrare sé stesso e di rispondere all'altro.

In questo scenario, l'etica della cura si offre come paradigma capace di colmare le lacune delle etiche puramente procedurali. Essa non muove da principi astratti, ma dall'esperienza concreta della vulnerabilità e della dipendenza reciproca. Prendersi cura significa riconoscere che l'autonomia non è autosufficienza, bensì possibilità sostenuta da relazioni.

Applicata alle nuove tecnologie digitali, l'etica della cura richiede sistemi progettati non solo per funzionare correttamente, ma per non ferire; non solo per essere efficienti, ma per essere giusti; non solo per decidere, ma per lasciare spazio alla contestazione, all'eccezione, alla storia individuale.

5.3.3 Narrazione, riconoscimento e responsabilità: l'importanza di un'etica nella progettazione

L'identità umana, radicata nell'essere personale, si esprime in una narrazione in divenire. Ogni individuo è più della somma delle sue tracce digitali, più del profilo che lo rappresenta. Quando i sistemi automatizzati congelano l'identità in classificazioni rigide, interrompono la continuità narrativa del sé. Un'etica autenticamente umana deve dunque preservare la possibilità del racconto, del cambiamento, del perdono e della revisione.

Progettare tecnologie responsabili significa assumere la responsabilità delle storie che esse rendono possibili o impossibili. Occorre perciò identificare valori chiave per la progettazione di sistemi di identità: benessere, autonomia, agency, uguaglianza, trasparenza, equità. Se si considera, ad esempio, la riflessione di Levinas, questa rafforza il valore della cura dell'altro, ricordando che la vulnerabilità è un tratto costitutivo dell'umano. Per Ricœur, essere sé stessi non significa restare immutati: la narrazione collega esperienze e cambiamenti nella continuità di una stessa vita **(Ricœur, 1990)**. Nel quadro personalista qui assunto, ciò illumina l'espressione temporale dell'unità della persona, senza fondarla nel racconto. La progettazione digitale deve quindi rispettare questa apertura, senza cristallizzare la persona nei dati del suo passato.

Per integrare la riflessione etica nella progettazione delle tecnologie sono disponibili diversi approcci e strumenti operativi, tra cui il *Value Sensitive Design* **(Friedman e Hendry, 2019)**, che invita a considerare i valori etici in tutte le fasi del design; il *Guidance Ethics Approach* **(GEA; Verbeek e Tijink, 2020)**, basato su workshop partecipativi che

coinvolgono stakeholder e comunità; l'*Ethics Canvas* **(Reijers et al., 2018)**, uno strumento visuale per mappare attori, valori, rischi e trade-off. Tali metodi possono inoltre essere arricchiti, come è giusto auspicarsi, dalle riflessioni di Levinas e Ricœur: un'attenzione sistematica alla vulnerabilità **(Levinas, 1961)**, una considerazione narrativa delle identità e dei contesti **(Ricœur, 1990)** e un approccio dialogico che valorizzi la pluralità delle prospettive.

L'identità digitale è un campo in cui si intrecciano tecnica, etica e politica. Un sistema realmente centrato sull'essere umano deve perciò riconoscere la vulnerabilità dell'altro, valorizzare la dimensione narrativa dell'identità e integrare valori e metodi etici in ogni fase della progettazione. Solo così sarà possibile costruire ecosistemi digitali che non solo funzionino, ma promuovano giustizia, dignità e inclusione.

Se questo è importante a livello di progettazione, lo è altrettanto sul piano di una consapevolezza più ampia delle questioni che riguardano la cura.

5.4 Bioetica, tecnica e potere: il rischio della società tecnocratica

L'accelerazione tecnologica che caratterizza il nostro tempo non è un mero fatto tecnico, ma un evento eminentemente politico e morale. Quando il sapere algoritmico diviene criterio privilegiato di decisione, e quando il controllo dei dati e delle infrastrutture digitali si concentra nelle mani di pochi attori, sia pubblici che privati, si profila il rischio di una società tecnocratica, nella quale il potere si esercita in forme opache, difficilmente contestabili e sempre meno partecipate. L'identità digitale ne è uno snodo decisivo: chi controlla le infrastrutture attraverso cui le persone vengono identificate e classificate dispone di un potere di definizione (§ 5.3.1) che sfugge in larga parte al controllo democratico.

In tale contesto, la crescente delega a sistemi automatizzati nei campi della sanità, del welfare, dell'istruzione e della sicurezza può generare un duplice impoverimento: da un lato, una riduzione della responsabilità umana; dall'altro, una progressiva erosione della legittimazione democratica. La riflessione bioetica impone qui una vigilanza critica: la tecnica deve rimanere strumento, mai istanza sovrana di giudizio.

5.4.1 Disuguaglianze digitali e ingiustizia algoritmica

Alle forme di esclusione digitale già esaminate sul piano giuridico (§ 3.1), legate all'età, alle condizioni economiche e alle competenze, si aggiunge un'ulteriore forma di ingiustizia: quella inscritta nei dati stessi. Dataset incompleti, distorti o non rappresentativi producono decisioni algoritmiche che amplificano pregiudizi preesistenti, colpendo in modo sproporzionato le popolazioni più vulnerabili.

In tale prospettiva, il principio di non discriminazione assume una funzione essenziale non solo sul piano etico, ma anche su quello giuridico, imponendo che i sistemi algoritmici siano progettati, valutati e monitorati in modo da prevenire effetti

discriminatori diretti o indiretti, soprattutto nei confronti delle persone in condizioni di vulnerabilità.

Un'etica autentica nel contesto contemporaneo non può dunque limitarsi a correggere ex post gli effetti discriminatori, ma deve interrogare le condizioni di produzione del sapere algoritmico, assumendo la giustizia e l'equità come criteri originari della progettazione.

5.4.2 Formazione, consapevolezza e cittadinanza digitale

In questo scenario, la formazione emerge come condizione di possibilità di ogni uso responsabile della tecnologia. Non è sufficiente apprendere competenze operative né agire solo a livello di progettazione: occorre sviluppare una comprensione critica dei dispositivi digitali, dei loro limiti epistemici e delle loro implicazioni etiche **(Fabris, 2025)**.

Una cittadinanza digitale matura è capace di difendere la propria autonomia informativa, riconoscere le forme di manipolazione e avvalersi delle tutele previste dalla normativa (artt. 22 GDPR e 86 *AI Act*; cfr. § 3.1) per ottenere spiegazioni e contestare le decisioni automatizzate. Sul piano etico, resta essenziale promuovere una comprensibilità dei processi decisionali e possibilità concrete di contestazione anche oltre le garanzie minime stabilite dalla legge, affinché la persona possa esercitare consapevolmente la propria autodeterminazione **(Fabris, 2025)**.

Analogamente, i professionisti, e in particolare quelli dei contesti di cura, devono essere formati a integrare sapere tecnico, sensibilità etica e competenza relazionale. Lungi dall'essere accessoria, la formazione diviene così un presidio di libertà. Essa consente anche di prendere consapevolezza di essere soggetti di diritti, il che implica riconoscere che non siamo solo i nostri dati: occorre perciò prestare attenzione a ciò che rendiamo visibile di noi stessi e, soprattutto, non appiattirci al contesto digitale nel quale siamo immersi.

5.4.3 La cura tra tecnica e relazione: contro la deumanizzazione

La medicina algoritmica promette diagnosi rapide e ottimizzazione delle risorse, ma la decisione clinica ultima deve rimanere una responsabilità umana non delegabile. Come argomentato nel capitolo 4 a proposito della relazione terapeutica, la tecnica deve arrestarsi di fronte alla fragilità costitutiva del paziente. Custodire l'umano nell'era digitale significa, in ultima analisi, erigere un presidio bioetico contro ogni forma di deumanizzazione, riaffermando che le vulnerabilità del corpo sofferente non sono un parametro da ottimizzare, ma il luogo in cui si radica l'irriducibile dignità della persona.

6. Prospettive future e proposte: verso una coesistenza equilibrata tra cambiamenti digitali e umanità

6.1 Come garantire una coesistenza equilibrata fra cambiamenti digitali e umanità

Se le riflessioni precedenti hanno mostrato come la tecnica, quando non è governata da una visione etica adeguata, possa trasformarsi da strumento di emancipazione in principio di dominio, è ora necessario volgere lo sguardo in avanti e interrogare il futuro non come destino già scritto, ma come campo aperto alla responsabilità dell'agire umano. Nulla, infatti, sarebbe più contrario allo spirito filosofico che rassegnarsi all'idea di un progresso automatico, come se la storia fosse guidata da una necessità impersonale e non dalle scelte degli uomini. Il futuro dei nuovi strumenti tecnologici non dipenderà soltanto dalla loro potenza computazionale, ma dalla capacità dell'umanità di orientarla secondo fini degni dell'uomo. La vera sfida non consiste nello scegliere tra entusiasmo acritico e rifiuto nostalgico, bensì nel costruire una coesistenza equilibrata, nella quale la tecnica sostenga la vita senza ridurla e amplifichi le possibilità umane senza svuotarle di senso.

Questo equilibrio non nasce dalla spontaneità del mercato né dall'autoregolazione dei sistemi tecnici, ma richiede un disegno consapevole, articolato e condiviso. In primo luogo, è necessaria una *governance* democratica della tecnologia, capace di sottrarre il potere algoritmico alla concentrazione oligarchica e di ricondurlo entro spazi di deliberazione pubblica, trasparente e inclusiva. Ciò implica anche la capacità delle Istituzioni di garantire che lo sviluppo e l'impiego dei sistemi digitali rimangano conformi ai principi dello Stato di diritto, assicurando la tutela effettiva dei diritti fondamentali.

In secondo luogo, nei processi decisionali che incidono sulla vita, sulla salute, sulla libertà e sulla dignità delle persone, occorre garantire una supervisione umana effettiva. La presenza di una persona nel processo decisionale (*human-in-the-loop*) è significativa solo se questa dispone delle competenze, delle informazioni e dell'autorità necessarie per valutare criticamente gli esiti del sistema, discostarsene e intervenire quando necessario. Il controllo ultimo deve restare umano, con responsabilità chiaramente attribuite, perché ogni decisione che incide sulla vita di una persona richiede qualcuno che ne risponda.

Infine, una coesistenza equilibrata richiede la valorizzazione di ciò che nessun algoritmo può sostituire: l'empatia, il giudizio prudenziale, la creatività, la responsabilità verso l'altro. Se la tecnica cresce, deve crescere insieme anche la consapevolezza del valore irriducibile della persona.

6.2 Il rischio di limiti etici inefficaci: verso un'etica della resistenza

Come si è già osservato (§§ 5.1-5.2), molti dei codici etici che oggi accompagnano lo sviluppo dei cambiamenti in atto rischiano di ridursi a esercizi retorici: solenni nelle dichiarazioni, deboli negli effetti. Quando l'etica si limita a ornare il discorso tecnologico senza incidere sulle pratiche reali, diventa non solo inefficace, ma complice. Si impone perciò la necessità di *un'etica della resistenza*. Resistere non significa opporsi al progresso, ma impedire che esso si trasformi in una forza cieca. Un'etica della resistenza esige strumenti concreti: meccanismi di controllo indipendenti dotati di reali poteri di intervento; forme di trasparenza radicale che rendano intelligibili non solo gli esiti, ma anche le logiche decisionali degli algoritmi; diritti effettivi alla spiegazione, alla contestazione e alla revisione umana delle decisioni automatizzate (cfr. § 3.1).

Si tratta, in altre parole, di passare da un'etica dei principi astratti a un'etica situata, capace di misurarsi con la specificità dei contesti in cui la tecnologia incide direttamente sulla vita delle persone; l'efficacia dell'etica dipende infatti dalla sua capacità di tradursi in responsabilità istituzionali, procedure verificabili e garanzie effettivamente esercitabili da parte delle persone.

In questa medesima direzione si muove la provocazione giuridica di Luca Bolognini **(Bolognini, 2018)** sul concetto di «follia artificiale». Di fronte alla tecnologizzazione e robotizzazione spinta dei rapporti umani, il giurista invoca la necessità di una vera e propria «resistenza dell'intelligenza umana». Se il tracciamento continuo e l'universo digitale tendono a imporre un'omologazione e un determinismo comportamentale, la resistenza etica e normativa deve configurarsi come la difesa dell'imprevedibilità, dell'imperfezione e del pensiero critico dell'individuo. La *governance* dell'innovazione deve quindi erigere barriere procedurali che tutelino non solo i dati, ma lo statuto stesso dell'umanità contro le derive di un'automazione che vorrebbe farsi istanza sovrana e totalizzante.

6.3 Orientamenti per integrare l'identità digitale nel concetto più ampio di persona

La digitalizzazione ha introdotto una trasformazione profonda nella comprensione dell'identità umana. Oggi la persona è anche rappresentata da dati, tracce digitali, profili e rappresentazioni algoritmiche. Il rischio, tuttavia, è che questa dimensione finisca per sovrapporsi all'interezza della persona, riducendola.

Integrare l'identità digitale nel concetto più ampio di persona significa riconoscere nella protezione dei dati personali una tutela della dignità e dell'autonomia. I diritti e le garanzie che la rendono effettiva, tra cui la trasparenza, la portabilità e la cancellazione dei dati, devono essere concretamente esercitabili secondo le condizioni previste dalla normativa. A questi strumenti giuridici di controllo e *accountability* deve affiancarsi la supervisione umana significativa, necessaria affinché l'innovazione tecnologica non comprometta l'autonomia decisionale e la specificità del soggetto.

Significa anche sviluppare una vera e propria antropologia digitale, capace di comprendere le trasformazioni psicologiche, sociali e culturali prodotte dalla vita mediata dagli algoritmi, senza smarrire il ruolo dell'essere umano come soggetto narrativo e responsabile.

6.4 Educazione digitale: formazione critica delle nuove generazioni e alfabetizzazione emotiva

Se il futuro sarà abitato da individui per i quali la distinzione tra *online* e *offline* sarà sempre più tenue, l'educazione digitale diventa una delle responsabilità più urgenti del nostro tempo. Non si tratta di aggiungere una disciplina tecnica ai curricula scolastici, ma di formare una competenza civica e culturale. Rispetto alla formazione di cittadini e professionisti già richiamata (§ 5.4.2), lo sguardo si rivolge qui in particolare alle nuove generazioni **(Leone XIV, 2026)**.

Educare digitalmente significa insegnare a leggere criticamente dati, algoritmi e piattaforme; riconoscere i *bias*; valutare le fonti; comprendere le dinamiche di manipolazione e polarizzazione. Significa inoltre promuovere un'alfabetizzazione emotiva che permetta di affrontare i rischi psicologici della vita digitale, dalla dipendenza alla perdita di senso.uniformalo

In questo senso, l'educazione digitale non è un investimento tecnologico, ma un investimento sulla libertà futura delle persone.

6.5 Il ruolo delle istituzioni, delle università e della società civile

Nessuna trasformazione di tale portata può essere governata da un solo attore. Per orientare lo sviluppo delle nuove tecnologie verso finalità autenticamente umane è necessaria un'alleanza ampia e responsabile.

Le istituzioni sono chiamate a definire quadri normativi chiari, nonché sistemi di vigilanza e valutazione capaci di monitorare nel tempo gli effetti dell'intelligenza artificiale sui diritti fondamentali e sull'equità dei servizi, aggiornati e realmente applicabili, capaci di proteggere i cittadini senza soffocare l'innovazione. Le università hanno il compito di formare professionisti competenti e consapevoli, promuovere la ricerca interdisciplinare e diffondere una cultura critica della tecnologia. La società civile, infine, deve partecipare attivamente al dibattito pubblico, vigilare sugli effetti della rivoluzione digitale e difendere i valori democratici nelle scelte tecnologiche.

Solo attraverso questa corresponsabilità sarà possibile costruire un ecosistema in cui la tecnologia non diventi strumento di dominio, ma mezzo di emancipazione.

Conclusioni

La coesistenza tra rivoluzione digitale e umanità non si configura come un problema tecnico da risolvere, bensì come uno spazio etico e politico da abitare in modo partecipativo. Le riflessioni sviluppate in questo documento hanno voluto dimostrare come la vera sfida non risieda nel rifiuto nostalgico o nell'entusiasmo acritico verso i nuovi strumenti, ma nella definizione delle condizioni antropologiche e giuridiche del loro impiego. La tecnologia, da sola, non garantisce progresso né giustizia; è l'essere umano, attraverso le proprie scelte valoriali, a orientarne il senso. L'approccio interdisciplinare qui adottato ha permesso di saldare lo sguardo filosofico della bioetica alla dogmatica giuridica, individuando nella relazione di cura e nella tutela costituzionale della persona i limiti invalicabili a qualunque riduzionismo algoritmico. Solo attraverso un dialogo costante tra sapere tecnico, filosofico e giuridico sarà possibile edificare una società digitale in cui l'identificazione rimanga un fattore di inclusione e cittadinanza, e mai un criterio di classificazione o depoliticizzazione della persona.

Si sta davvero compiendo un passaggio dalla persona all'identità digitale? La risposta che emerge è negativa, ma non rassicurante. Sul piano ontologico tale passaggio non può avvenire: la persona, unità psichica, spirituale e corporea, possiede una dignità che nessuna rappresentazione può conferire o togliere, e l'identità digitale ne resta una rappresentazione parziale, utile e talvolta necessaria, legittima solo finché rimane al suo servizio. Sul piano pratico, tuttavia, la sostituzione può avvenire di fatto, senza essere mai dichiarata: quando profili, credenziali e inferenze diventano il criterio con cui si accede ai diritti, alla partecipazione democratica e alla cura. Custodire il primato della persona significa allora vigilare su questo scarto, con lo sguardo della bioetica e con gli strumenti del Diritto, e praticare, quando necessario, quell'etica della resistenza di cui si è detto.

Non è infatti la grandezza dei mezzi a rendere giusta una civiltà, ma la saggezza con cui essa sceglie i propri fini.

Riferimenti bibliografici

ARENDT H., *The Human Condition*, University of Chicago Press, Chicago 1958 (trad. it. *Vita activa. La condizione umana*, Bompiani, Milano 2019).

BOLOGNINI L., *Follia artificiale. Riflessioni per la resistenza dell'intelligenza umana*, Rubbettino Editore, Soveria Mannelli 2018.

BOLOGNINI L. (a cura di), *Privacy e libero mercato digitale. Convergenza tra regolazioni e tutele individuali nell'economia data-driven*, Giuffrè Francis Lefebvre, Milano 2021.

FABRIS A., *La filosofia nell'epoca dell'intelligenza artificiale. Come ci aiuta a vivere in ambienti tecnologici*, Carocci, Roma 2025.

FLORIDI L., *The Philosophy of Information*, Oxford University Press, Oxford 2011 (trad. it. *Filosofia dell'informazione*, Raffaello Cortina Editore, Milano 2024).

FLORIDI L., *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford University Press, Oxford 2014 (trad. it. *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano 2017).

FLORIDI L. (a cura di), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer, Cham 2015.

FOUCAULT M., *Surveiller et punir: Naissance de la prison*, Gallimard, Paris 1975 (trad. it. *Sorvegliare e punire. Nascita della prigione*, Einaudi, Torino 2014).

FRIEDMAN B., HENDRY D.G., *Value Sensitive Design: Shaping Technology with Moral Imagination*, MIT Press, Cambridge (MA) 2019.

GOFFMAN E., *The Presentation of Self in Everyday Life*, Anchor Books, Garden City (NY) 1959 (trad. it. *La vita quotidiana come rappresentazione*, il Mulino, Bologna 1997).

HABERMAS J., *Faktizität und Geltung*, Suhrkamp, Frankfurt am Main 1992 (trad. it. *Fatti e norme. Contributi a una teoria discorsiva del diritto e della democrazia*, Guerini e Associati, Milano 1996).

HAN B.-C., *Psychopolitik: Neoliberalismus und die neuen Machttechniken*, S. Fischer Verlag, Frankfurt am Main 2014 (trad. it. *Psicopolitica*, nottetempo, Milano 2016).

LEONE XIV, *Magnifica humanitas. Lettera enciclica sulla custodia della persona umana nel tempo dell'intelligenza artificiale*, Santa Sede, Città del Vaticano, 15 maggio 2026.

LEVINAS E., *Totalité et Infini: Essai sur l'extériorité*, Martinus Nijhoff, La Haye 1961 (trad. it. *Totalità e Infinito. Saggio sull'esteriorità*, Jaca Book, Milano 1980).

MERLEAU-PONTY M., *Phénoménologie de la perception*, Gallimard, Paris 1945 (trad. it. *Fenomenologia della percezione*, Bompiani, Milano 2003).

REIJERS W., KOIDL K., LEWIS D., PANDIT H.J., GORDIJN B., *Discussing Ethical Impacts in Research and Innovation: The Ethics Canvas*, in KREPS D., ESS C., LEENEN L., KIMPPA K. (a cura di), *This Changes Everything – ICT and Climate Change: What Can We Do?*, IFIP Advances in Information and Communication Technology, vol. 537, Springer, Cham 2018, pp. 299-313.

RICŒUR P., *Soi-même comme un autre*, Seuil, Paris 1990 (trad. it. *Sé come un altro*, Jaca Book, Milano 1993).

RICŒUR P., *Les trois niveaux du jugement médical*, in «Esprit», 227(12), 1996, pp. 21-33.

RICŒUR P., *Parcours de la reconnaissance: Trois études*, Stock, Paris 2004 (trad. it. *Percorsi del riconoscimento*, Raffaello Cortina Editore, Milano 2005).

RODOTÀ S., *Tecnologie e diritti*, il Mulino, Bologna 1995.

RODOTÀ S., *Dal soggetto alla persona*, Editoriale Scientifica, Napoli 2007.

VERBEEK P.-P., TIJINK D., *Guidance Ethics Approach: An Ethical Dialogue about Technology with Perspective on Actions*, ECP | Platform voor de InformatieSamenleving, Den Haag 2020.

ZUBOFF S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York 2019 (trad. it. *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Luiss University Press, Roma 2019).