Rivista elettronica di Diritto, Economia, Management

Numero 3 - 2025

# La "Dichiarazione europea sui principi e diritti digitali" - Per il decennio digitale 2020-2030

## A cura di Donato A. Limone

Inquadra il QR-CODE per il download degli altri numeri della Rivista

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOEDU®

ISSN 2039-4926

*La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente, che ha lo scopo di trattare le diverse tematiche giuridiche, economiche e manageriali con un approccio integrato e trasversale, di tipo comparato, in un contesto locale, nazionale, comunitario ed internazionale caratterizzato dalla società dell'informazione, dalla trasformazione digitale, dalla globalizzazione dei mercati, da processi innovativi di tipo manageriale ed organizzativo nei settori pubblico e privato.*
*La rivista ha anche la finalità di ospitare contributi di giovani studiosi per valorizzarne le attitudini alla ricerca e il loro contributo allo sviluppo delle scienze giuridiche, sociali, economiche e manageriali.*



**Direzione e redazione:** Via Riccardo Grazioli Lante, 15 – 00195 Roma - *donato.limone@gmail.com*

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno XV, n. 3/2025
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce



**Codice etico:** *www.clioedu.it/rivistaelettronica#codice-etico*
**Procedure di referaggio:** *www.clioedu.it/rivistaelettronica#referaggio*
**Elenco dei numeri pubblicati:** *www.clioedu.it/rivistaelettronica*

# INDICE

N. 3 - 2025 - pp. 3-6

# Editoriale

Con questo numero monografico dedicato alla ***"Dichiarazione europea sui diritti e principi digitali"*** chiudiamo la serie dei numeri specialistici dell'anno 2025.

Abbiamo pubblicato infatti i seguenti numeri monografici di rilevante attualità:
**N. 2/2025**: Biblioteche e trasformazione digitale. A cura di Rosa Maiello.
**N. 1/2025**: NIS 2 e Cybersecurity. A cura di Sarah Ungaro.

Con il presente fascicolo intendiamo pubblicare una serie di contributi a commento della "Dichiarazione" con considerazioni da parte di approcci diversi: istituzionale, normativo, organizzativo, strategico, tecnico.

La "Dichiarazione" costituisce la "Carta digitale" della UE con riferimento al decennio digitale.

È una "Carta" importante perché definisce una strategia di sviluppo del digitale europeo: la Carta è scritta in modo chiara, comprensibile da parte di tutti, completa, con un linguaggio essenziale ed asciutto, con indicazione delle tematiche caratterizzanti la stessa politica UE del settore e delle cose da fare (impegni della UE rispetto alla Carta).

Abbiamo dedicato un numero specifico al tema perché della Dichiarazione in Italia si è parlato molto poco ed è un documento che non viene utilizzato di fatto nella definizione delle politiche italiane del settore (a livello parlamentare, governativo, ministeriale, dipartimentale).

Rileviamo come i principi e di diritti digitali della "Dichiarazione" sono stati "anticipati" dal Codice dell'amministrazione digitale (dlgs 82/2005 e sm) e nella fase di attuazione dello stesso Codice sono stati resi esecutivi ed attuati anche tramite il sistema delle regole tecniche e delle linee guida Agid.

La Carta ha particolare rilevanza se la consideriamo nel decennio digitale 2020-2030 in merito alla attuazione delle direttive e dei regolamenti sulla Intelligenza artificiale, su eIDAS 1 e 2, sulla governance dei dati nel settore pubblico e privato, sullo sviluppo dei mercati digitali e del commercio elettronico, della cibersicurezza, della protezione dei dati personali, dello sviluppo di una cultura dei dati di qualità messi a disposizione in "spazi comuni europei" per creare una cultura dei dati europei.

I contributi di questo numero:

Donato Limone (*La Dichiarazione europea sui principi e diritti digitali. Considerazioni introduttive*): struttura della Dichiarazione, applicazioni, monitoraggio.

Marco Bussone (*Digitale strumento di unità e di comunità*): ogni giorno, ci interroghiamo su come le comunità siano più digitali, e più connesse, tra loro e con le altre. Si parte dalle infrastrutture. Una questione europea, sancita dalla Carta dei diritti e principi digitali del decennio digitale. Connessi tra noi e con gli altri. È un grave problema che il piano banda ultralarga sia in ritardo di quattro anni, perché il cerino resta nelle mani dei sindaci con i cittadini arrabbiati. Dobbiamo evitare che la burocrazia distrugga le buone cose che si sono fatte, ovvero che lo Stato possa intervenire laddove l'infrastruttura non c'è.

L'articolo Di Massimo Farina "*Governance algoritmica dei principi digitali europei: modelli e prospettive".* Ha lo scopo di analizzare la regolamentazione tecnologica.

Andrea Lisi e Sarah Ungaro (*L'architettura normativa dei diritti digitali nella Dichiarazione europea per il decennio digitale: principi fondamentali e nuove regolamentazioni nel quadro di un costituzionalismo digitale europeo)* analizzano attraverso un approccio analitico rigoroso, i contenuti e le implicazioni giuridiche dei capitoli III e V della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, adottata il 15 dicembre 2022 dalle istituzioni dell'Unione Europea. L'indagine si concentra sulla complessa articolazione tra libertà di scelta nell'ecosistema digitale e sicurezza, protezione e conferimento di maggiore autonomia responsabile, evidenziando le tensioni dialettiche e le sfide ermeneutiche che connotano l'implementazione di tali principi nella prassi giuridica contemporanea.

Giovanni Manca (*La reale attuazione di principi e diritti digitali in Italia):* La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01) è fondamentale per orientare le scelte di natura sociale per un mondo che è già ampiamente digitale e con l'intelligenza artificiale tende a esserlo ancora di più occupando gli spazi della persona. L'espressione diritti digitali è anche seducente, se il mondo è digitale anche la persona deve disporre e reclamare i propri diritti.In Italia a partire dai primi anni '90 la legislatura ha sempre di più sviluppato il tema di amministrazione digitale della società. Una indiscutibile pietra miliare è il Codice dell'amministrazione digitale (CAD – Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni) che peraltro, nel tempo ha perso l'obiettivo di essere principio, scivolando sempre di più verso lo stato di contenitore di norme, anche attuative, da inserire "al volo" per legiferare sui temi del momento. Alla data di marzo 2025 il sito di Normattiva ci informa che sono 509 le modifiche rispetto al testo originale.

Paolo De Nardis, Stefano Epifani, Matteo Bozzoli (*La sostenibilità digitale come elemento abilitante di cittadinanza):* gli Autori fanno una riflessione generale sul decennio digitale europeo (2020-2030), delineato dalla Commissione Europea attraverso la comunicazione "2030 Digital Compass", mira a costruire un futuro digitale sostenibile, inclusivo e competitivo per l'Europa. Tra gli obiettivi prioritari figurano

la promozione delle competenze digitali, la realizzazione di infrastrutture digitali sicure e sostenibili, la digitalizzazione delle imprese e la trasformazione dei servizi pubblici. Questi pilastri sono centrali per una crescita economica equa, resiliente e inclusiva, basata su una solida cultura digitale e su tecnologie orientate al bene comune.

Il contributo di Enzo Chilelli (Gli USA inventano, la Cina copia e l'Europa norma…..) una riflessione sulla transizione digitale.

Il Contributo di Daniele Napoleone (*La dichiarazione sui diritti e principi digitali per il decennio digitale: una costituzione digitale per l'Europa. Opportunità e rischi di un'interpretazione solamente formale*). La Dichiarazione europea rappresenta un atto politico che delinea una visione comune per guidare la trasformazione digitale dell'Europa nel rispetto dei diritti fondamentali e dei valori democratici. Pur non essendo vincolante, essa si configura come una "costituzione digitale" capace di orientare le politiche nazionali. Tuttavia, il rischio di una ricezione meramente formale è concreto, soprattutto in Paesi come l'Italia, dove spesso le misure sono state adottate in ottica di adempimento burocratico. L'articolo propone di interpretare la Dichiarazione non come un elenco di principi astratti, ma come un quadro operativo da tradurre in politiche concrete, fondate su sostenibilità economica e organizzativa, cooperazione territoriale, valorizzazione delle competenze e strumenti di valutazione dell'impatto. Solo in questo modo essa può diventare una bussola per un digitale europeo realmente a misura di cittadino.

Enrica Priolo (*Il paradigma europeo della sicurezza digitale tra security by design e autodeterminazione informazionale: riflessioni critiche sul Capitolo V della Dichiarazione europea sui diritti e principi digitali.)* La Dichiarazione europea sui diritti e principi digitali per il decennio digitale configura un modello di governance tecnologica che tenta di conciliare le esigenze di sicurezza sistemica con l'autodeterminazione individuale. Il contributo analizza criticamente il paradigma "sicurezza-protezione-responsabilizzazione" delineato nel Capitolo V, evidenziandone le implicazioni giuridico-economiche e le tensioni dialettiche tra tutela eteronoma e autonomia soggettiva nell'ecosistema digitale europeo, con particolare attenzione alle criticità emergenti dal binomio empowerment/marketing digitale.

Di Alessia Palladino *(Il decennio digitale nella sanità "virtuale": il caso del metaverso):* Un contributo su di un tema specifico trattato dalla Dichiarazione.

Il Direttore della Rivista
*Donato A. Limone*

N. 3 - 2025 - pp. 6-16

# Dichiarazione europea sui diritti e principi digitali". Una "Carta" per la strategia europea sul "digitale" (2020-2030)

**Donato A. Limone**

**Abstract:** La "Dichiarazione sui principi e diritti digitali" (2023): struttura, applicazioni, monitoraggio.

European Declaration on Digital Rights and Principles for the Digital Decade (2023): Structure, Applications, and Monitoring

**Parole chiave**: Dichiarazione, Carta, diritti digitali, principi digitali, strategia europea, applicazioni, monitoraggio.



## 1. Premessa

Con il presente fascicolo intendiamo pubblicare una serie di contributi a commento della "Dichiarazione" con considerazioni di tipo istituzionale, normativo, organizzativo, strategico, tecnico.

La *"Dichiarazione"* costituisce la *"Carta digitale"* della UE con riferimento al decennio digitale 2020-2030.

È una *"Carta"* importante perché definisce una strategia di sviluppo del digitale europeo con una "visione" a supporto della stessa strategia: la *Carta* è scritta in modo chiara, comprensibile da parte di tutti, completa, con un linguaggio essenziale ed asciutto, con indicazioni specifiche delle tematiche caratterizzanti la stessa politica UE del settore e delle cose da fare (impegni della UE rispetto alla Carta).

Della *Dichiarazione* in Italia si è parlato molto poco ed è un documento che non viene utilizzato di fatto nella definizione delle politiche italiane del settore (a livello parlamentare, governativo, ministeriale, dipartimentale).

Rileviamo come i principi e di diritti digitali della *"Dichiarazione"* (2023) sono stati "anticipati" in Italia dal Codice dell'amministrazione digitale (dlgs 82/2005 e sm) e nella fase di attuazione dello stesso *Codice* e sono stati resi esecutivi ed attuati anche tramite il sistema delle regole tecniche e delle linee guida Agid. *Allo stato attuale in Italia non possiamo contare né sua di una "visione" sul digitale né su di una strategia specifica ed operativa: ci troviamo di fronte ad documenti generici, frammenti di visione e di strategia che non hanno alcun valore; lo stesso PNRR è la "scomposta composizione" di progetti a volte senza senso e finalità e con scarso valore di efficacia progettuale (ce ne renderemo conto nel 2026 quando si farà la "rendicontazione" vera, con parametri oggettivi; fuori dalla logica del pagamento delle rate PNRR pagate senza una valutazione progettuale complessiva ma soprattutto, economica, tecnica, per verificare l'efficacia dei diversi interventi/pagamenti sui processi di trasformazione digitale, innovazione organizzativa ed amministrativa, sui servizi digitali ai cittadini e alle imprese, ecc.*

La Carta ha particolare rilevanza se la consideriamo nel decennio digitale 2020-2030 in merito alla attuazione delle direttive e dei regolamenti sulla Intelligenza artificiale, su eIDAS 1 e 2, sulla governance dei dati nel settore pubblico e privato, sullo sviluppo dei mercati digitali e del commercio elettronico, della cibersicurezza, della protezione dei dati personali, dello sviluppo di una cultura dei dati di qualità messi a disposizione in "spazi comuni europei" per creare una cultura dei dati europei.

# 2. Il contesto europeo per lo sviluppo del digitale

Dal 2020 la strategia europea per lo sviluppo del digitale nei Paesi della Unione ha fatto registrare un salto di qualità con una serie di interventi politici e normativi di particolare rilevanza.

## 2.1 Il decennio digitale europeo 2030

Il programma strategico per il decennio digitale comprende gli obiettivi del decennio, i progetti multinazionali e i diritti e principi del decennio digitale:

- Gli obiettivi del decennio digitale sono obiettivi misurabili per ciascuna delle quattro aree: connettività, competenze digitali, imprese digitali e servizi pubblici digitali.
- Gli obiettivi del decennio digitale guideranno le azioni degli Stati membri. La Commissione informerà le azioni degli Stati membri nella relazione annuale.
- Il programma strategico per il decennio digitale consentirà all'UE e agli Stati membri di collaborare per raggiungere gli obiettivi del decennio digitale e i suoi obiettivi. Esso stabilisce un meccanismo per monitorare i progressi compiuti verso il 2030. Ogni anno la Commissione pubblicherà una relazione per fare il punto sui progressi compiuti.
- I progetti multinazionali consentiranno agli Stati membri di mettere in comune gli investimenti e avviare progetti transfrontalieri su larga scala.
- I diritti e i principi del decennio digitale riflettono i valori dell'UE, che devono essere rispettati nel mondo digitale.

Gli obiettivi principali possono essere riassunti in 4 punti:

1. una popolazione digitalmente qualificata e professionisti digitali altamente qualificati;
2. infrastrutture digitali sicure e sostenibili;
3. trasformazione digitale delle imprese;
4. digitalizzazione dei servizi pubblici.

## 2.2. La Dichiarazione europea sui diritti e principi digitali per il decennio digitale

La Dichiarazione, proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione, è stata pubblicata sulla Gazzetta Ufficiale dell'Unione Europea del 23.1.2023 (C 23/1).

Nei primi 4 considerando del Preambolo (che riportiamo) sono indicati con chiarezza e completezza i fondamenti sui quali si basa la Dichiarazione:

(1) L'Unione europea (UE) è un'«unione di valori», sancita dall'articolo 2 del trattato sull'Unione europea, e si fonda sul rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e sul rispetto

dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Inoltre, secondo la Carta dei diritti fondamentali dell'Unione europea, l'UE si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà. La Carta ribadisce inoltre i diritti derivanti in particolare dagli obblighi internazionali comuni agli Stati membri.

(2) La trasformazione digitale interessa ogni aspetto della vita delle persone. Offre notevoli opportunità in termini di miglioramento della qualità della vita, crescita economica e sostenibilità.

(3) La trasformazione digitale presenta anche sfide per le nostre società democratiche e le nostre economie, così come per gli individui. Con l'accelerazione della trasformazione digitale è giunto il momento che l'UE specifichi come si dovrebbero applicare nell'ambiente digitale i suoi valori e diritti fondamentali applicabili offline. La trasformazione digitale non dovrebbe comportare la regressione dei diritti. Ciò che è illegale offline è illegale online. La presente dichiarazione non pregiudica le «politiche offline», come l'accesso offline ai servizi pubblici principali.

(4) Il Parlamento ha invitato più volte a definire principi etici che guidino l'approccio dell'UE alla trasformazione digitale e garantiscano il pieno rispetto dei diritti fondamentali quali la protezione dei dati, il diritto al rispetto della vita privata, la non discriminazione e la parità di genere, nonché di principi quali la protezione dei consumatori, la neutralità tecnologica e della rete, l'affidabilità e l'inclusività. Ha inoltre chiesto una maggiore protezione dei diritti degli utenti nell'ambiente digitale, nonché dei diritti dei lavoratori e del diritto alla disconnessione".

I principi della Dichiarazione sono modellati intorno a 6 temi:

1. *Mettere le persone e i loro diritti al centro della trasformazione digitale*
2. *Sostenere la solidarietà e l'inclusione*
3. *Garantire la libertà di scelta online*
4. *Promuovere la partecipazione allo spazio pubblico digitale*
5. *Aumentare la sicurezza, la sicurezza e l'empowerment delle persone*
6. *Promuovere la sostenibilità del futuro digitale*

***Mettere le persone al centro della trasformazione digitale (Capitolo I)***

Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali.

***Solidarietà e inclusione (Capitolo II)***

La tecnologia dovrebbe essere utilizzata per unire le persone, e non per dividerle.

Tutti dovrebbero avere accesso alla tecnologia, che dovrebbe essere inclusiva, e promuovere i nostri diritti. La dichiarazione propone diritti in una serie di settori chiave per garantire che nessuno sia lasciato indietro dalla trasformazione digitale, assicurando uno sforzo supplementare per includere gli anziani, le persone che vivono nelle zone rurali, le persone con disabilità e le persone emarginate, vulnerabili o prive di diritti e coloro che agiscono per loro conto.
Concretamente, i firmatari si impegneranno ad agire in una serie di settori, tra cui: connettività; istruzione, formazione e competenze digitali; condizioni di lavoro eque e giuste; servizi pubblici digitali.
Ogni persona dovrebbe avere accesso online ai servizi pubblici principali nell'UE. A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo.

***Libertà di scelta (Capitolo III)***
Promuovere sistemi di IA antropocentrici, affidabili ed etici.
Nell'uso di sistemi di IA garantire un livello adeguato di trasparenza.
I sistemi di IA devono contribuire a creare ed aumentare il benessere e non devono creare condizioni discriminanti.
Ognuno dovrebbe avere il potere di fare le proprie scelte informate online.
La libertà di scelta include anche l'essere liberi di scegliere quali servizi online utilizziamo, sulla base di informazioni oggettive, trasparenti e affidabili. Questo a sua volta significa assicurarsi che tutti abbiano il potere di competere e innovare nel mondo digitale.

***Partecipazione allo spazio pubblico digitale (Capitolo IV)***
Le tecnologie digitali possono essere utilizzate per stimolare l'impegno e la partecipazione democratica. Tutti dovrebbero avere accesso a un ambiente online affidabile, diversificato e multilingue e dovrebbero sapere chi possiede o controlla i servizi che stanno utilizzando. Ciò incoraggia il dibattito pubblico pluralistico e la partecipazione alla democrazia.
I principi digitali sottolineano inoltre la necessità di creare un ambiente digitale che protegga le persone dalla disinformazione, dalla manipolazione delle informazioni e da altre forme di contenuti dannosi, comprese le molestie e la violenza di genere. Inoltre, supporta l'accesso a contenuti digitali che riflettono la nostra diversità culturale e linguistica.

***Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità (Capitolo V)***
Tutti dovrebbero avere accesso a tecnologie, prodotti e servizi digitali sicuri, protetti dalla privacy. I principi digitali si impegnano a proteggere gli interessi delle persone, delle imprese e dei servizi pubblici contro la criminalità informatica e a confrontarsi con coloro che cercano di minare la sicurezza e l'integrità del nostro ambiente online.

La dichiarazione invita tutti ad avere un controllo effettivo sui propri dati personali e non personali in linea con il diritto dell'UE. Presta particolare attenzione ai bambini e ai giovani, che dovrebbero sentirsi al sicuro e potenziati online.

***Sostenibilità (Capitolo VI)***
Le transizioni digitale e verde sono strettamente collegate. Mentre le tecnologie digitali offrono molte soluzioni per i cambiamenti climatici, dobbiamo garantire che non contribuiscano al problema stesso. I prodotti e i servizi digitali dovrebbero essere progettati, prodotti e smaltiti in modo da ridurne l'impatto sull'ambiente e sulla società. Dovrebbero inoltre essere fornite maggiori informazioni sull'impatto ambientale e sul consumo energetico di tali servizi.

*Abbiamo sottolineato, in sintesi, alcuni elementi significativi della Dichiarazione che costituisce quindi una "linea guida fondamentale" per lo sviluppo non solo del decennio digitale europeo (anche in chiave di sviluppo delle imprese del settore) ma anche per tutta la relativa regolamentazione del settore e soprattutto per contribuire allo sviluppo di una cultura digitale moderna.*

# 3. Le nuove burocrazie pubbliche nell'epoca digitale: dalle tecnologie ai dati attraverso nuovi modelli organizzativi

Il triennio 2022-2024 può essere considerato senza dubbio il periodo di svolta nel sistema regolatorio europeo del "digitale" sia per quanto attiene le "tecnologie" sia per quanto attiene la cultura e la gestione dei "dati" con un approccio (finalmente) sistemico ed integrato. E per la trasformazione digitale del settore pubblico questo triennio può significare l'avvio di un reale processo di innovazione e di cambiamento, con particolare riferimento alle burocrazie pubbliche. Questa nuova fase è scandita da alcuni atti regolatori che possiamo considerare fondamentali e che si riferiscono a:

- Governance europea dei dati;
- Intelligenza Artificiale;
- Identità digitale europea e servizi digitali (eIDAS).

Governance dei dati significa qualità dei dati; una nuova cultura dei dati e del loro valore sociale, economico, amministrativo; "apertura" dei dati pubblici.

Intelligenza Artificiale: un insieme di regole comuni per i Paesi della UE al fine

di “innovare” nel rispetto di principi etici, dei diritti umani, dello stato di diritto, della Carta dei diritti fondamentali dell’UE.

eIDAS: un sistema di servizi basati su di una identità digitale europea, certa, sicura, interoperabile per servizi pubblici e privati accessibili senza vincoli di eccessiva “intermediazione” amministrativa o gestionale per l’accesso e per le attività amministrative e/o per i mercati e le professioni.

Il regolamento eIDAS nel settore pubblico costituirà un modo nuovo di “fare amministrazione”, con una forte semplificazione dei dati e dei processi amministrativi, con la eliminazione di “ridondanze” di dati/procedure/processi, con una accessibilità “diretta” ed in modalità nativamente digitale ai servizi pubblici.

Il regolamento eIDAS (se letto ed attuato come un “nuovo paradigma di innovazione amministrativa”) costituisce la “dimensione” giusta per una evoluzione verso nuovi modelli organizzativi delle pubbliche amministrazioni.

In questo articolo intendiamo contribuire alla formazione di una nuova visione dei rapporti “cittadino/amministrazione” consapevoli che nessuna ulteriore riforma della pubblica amministrazione sarà possibile (sia pure con il rispetto dei criteri classici dell’amministrare: efficienza, efficacia, trasparenza, economicità, partecipazione, sostenibilità, ecc.) al di fuori di un contesto stabilito dai principi di eIDAS (identità digitale, accessibilità piena in rete, fruizione di servizi digitali). Questi principi nel nostro Paese sono stati anticipati dal Codice dell’amministrazione digitale, 2005 e sm) che però resta un sistema regolatorio ampiamente “disapplicato” nella sua organicità.

È necessario anche considerare il “contesto nazionale” nel quale questi sistemi regolatori devono operare.

# 4. L’innovazione digitale nel settore pubblico italiano “rinviata”, “bloccata”, senza una “strategia”: il contesto nazionale

Quale è il contesto nel quale i sistemi regolatori della UE hanno iniziato ad operare? È necessario partire da una considerazione generale.

La trasformazione digitale comprende sia processi di riorganizzazione e sia

aspetti tecnologici. Le pubbliche amministrazioni dovrebbero applicare l'art. 15 del Codice dell'amministrazione digitale (prima riorganizzare e poi digitalizzare). Oggi le P.A. operano in una perpetua condizione di "dicotomia" (organizzazioni pubbliche, da un lato, che non si mettono mai in discussione e le tecnologie, dall'altro, che sono applicate per lo più nella logica strumentale).

Se non si supera questa dicotomia (organizzazione e tecnologia) e non si procede con un approccio sistemico siamo di fronte a processi di automazione e non di trasformazione digitale. Non siamo di fronte a processi di innovazione amministrativa e tecnologica.

L'attuale contesto della trasformazione digitale nelle PA conferma:

- che le P.A. operano sulla base di modelli organizzativi superati
- che le P.A. non hanno proceduto ad effettuare interventi di radicale semplificazione delle procedure, dei procedimenti e dei processi amministrativi
- che abbastanza poco significativo è il livello di sviluppo di servizi in rete di qualità (art. 7 del CAD)
- che l'attuazione delle regole tecniche (Agid) in materia di formazione, gestione, conservazione dei documenti ha interessato pochissime amministrazioni pubbliche
- che non si rilevano sistematicamente i bisogni dei servizi per i cittadini e la soddisfazione di questi per i servizi stessi
- che non c'è una cultura sulla governance e la qualità dei dati, delle informazioni, dei sistemi informativi pubblici
- che se la formazione del personale delle PA è quasi residuale, la formazione sui processi innovativi e di cambiamento è tendente allo zero
- critica è la situazione sulla sicurezza informatica.

Un contesto poco significativo, povero di stimoli per il cambiamento, oggi ricco di risorse (PNRR) a rischio perché nel 2026 questo Piano andrà in chiusura e con quali risultati concreti ed efficaci?

Il ricco quadro delle regole della UE si inizia a strutturare con il regolamento 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati). Sempre sui dati viene approvato il regolamento UE (Data Act) n. 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

Nel 2023 viene proclamata la Dichiarazione europea sui diritti e i principi digitali. Nel 2024 sono approvati i regolamenti sulla IA e su eIDAS. Il regolamento su IA

molto discusso e partecipato in sede politica europea (oggi “commentato” quotidianamente dalla maggior parte dei media, con pochi  interventi interessanti, ben scritti e finalizzati a creare una cultura sulla “civiltà delle macchine”). Pochissime nicchie di mercati europei e italiani; quasi esclusivamente mercato statunitense. Per fortuna ci sono alcuni poli universitari di ricerca italiani che operano bene ed in silenzio fuori dalle logiche mediatiche.

Il regolamento eIDAS ( più tecnico) è tutto da scoprire sotto il profilo non solo tecnico ma anche sotto il profilo delle definizioni, della integrazione tra identità digitali europee, utilizzo di attributi personali, di cibersicurezza. Noi intendiamo offrire una chiave di lettura che ci permetta di valutare l’impatto di eIDAS sulla P.A. intesa come ecosistema amministrativo digitale. Il regolamento eIDAS come sistema di “valori amministrativi” visti nel loro insieme: sistema di dati e processi; sistema di servizi; integrazione di identità digitale, processi, fruizione di servizi; nuovi modelli tecno-amministrativi; qualità dell’amministrare, dei servizi, per un novo rapporto cittadino/stato (rinvio all’unico organico strumento di analisi su eIDAS costituito dal fascicolo n.4/2024 della “Rivista elettronica di diritto, economia, management”, fascicolo curato da un grande specialista della materia, Giovanni Manca; https://www.clioedu.it/marketplace/elenco-completo/item/n-2024-4-rivista-elettronica-di-diritto-economia-management).

# 5. Applicazioni dei principi della Dichiarazione

I principi della Dichiarazione implicano concretamente, in sintesi, quanto segue:

- Connettività accessibile: Tutti dovrebbero avere accesso a una connessione digitale ad alta velocità.
- Competenze digitali: È fondamentale fornire a tutti l’istruzione e la formazione necessarie per acquisire competenze digitali.
- Servizi pubblici online: I cittadini devono poter accedere ai servizi pubblici principali online.
- Protezione dei minori: Deve essere garantito un ambiente digitale sicuro per i bambini e i giovani.
- Controllo dei dati: Le persone devono avere un controllo effettivo sui propri dati personali.
- Diritto alla disconnessione: La possibilità di disconnettersi dal lavoro dopo l'orario.
- Trasparenza ambientale: Informazioni comprensibili sull’impatto ambientale dei prodotti digitali.

- Libertà di espressione: Salvaguardare la libertà di espressione e informazione online.
- Intelligenza Artificiale al servizio delle persone: L'IA deve essere uno strumento per il benessere umano, non uno strumento di controllo.

# 6. Il monitoraggio dell'applicazione della "Dichiarazione"

La Commissione si è impegnata a monitorare, annualmente, l'applicazione dei diritti e dei principi digitali in tutta l'UE.

Il rapporto esamina anche l'attività degli Stati membri e l'impatto delle loro iniziative in modo più quantitativo. La panoramica dell'UE dei 27 Paesi è integrata da un'analisi specifica per paese, parte delle relazioni nazionali sullo Stato del Decennio Digitale.

I risultati del rapporto traggono spunto da diverse fonti, tra cui:

- Uno studio indipendente commissionato dalla Commissione europea, che ha raccolto ulteriori contributi dagli Stati membri, dall›industria e dalla società civile
- L'indice dell'economia e della società digitale (DESI)
- Vari meccanismi di segnalazione della Commissione e di altro tipo
- Il rapporto speciale dell'Eurobarometro 2025 sul decennio digitale, che offre una panoramica della percezione delle persone riguardo ai diritti e ai principi digitali.
- La relazione si presenta come un documento di lavoro dei servizi che integra l'analisi dei progressi verso gli obiettivi e i traguardi del decennio digitale presentata nel rapporto sullo stato del decennio digitale 2025.

*Non intendiamo, in questa sede, discutere in dettaglio i risultati del monitoraggio 2025 della UE sulla attuazione della "Dichiarazione" che invece saranno presi in esame nel prossimo numero della "Rivista".*

Ci limitiamo per il momento a rinviare alla documentazione ufficiale sintetica pubblicata da fonti ufficiali:

1. Comunicazione della Commissione "Stato del decennio digitale 2025: conti-

nuare a costruire la sovranità e il futuro digitale dell'UE" (relazione principale) - Scaricamento

2. Allegato 1 - Stato della trasformazione digitale dell'UE nel 2025: progressi e raccomandazioni orizzontali - Scaricamento
3. Una analisi sintetica sulla Italia (17 - Breve rapporto nazionale sull'Italia Scaricamento ).

N. 3 - 2025 - pp. 17-20

# Digitale strumento di unità e di comunità

**Marco Bussone**
*Presidente nazionale Uncem*
*Unione nazionale Comuni Comunità Enti montani*

Ogni giorno, ci interroghiamo su come le comunità siano più digitali, e più connesse, tra loro e con le altre. Si parte dalle infrastrutture. Una questione europea, sancita dalla Carta dei diritti e principi digitali del decennio digitale. Connessi tra noi e con gli altri. È un grave problema che il piano banda ultralarga sia in ritardo di quattro anni, perché il cerino resta nelle mani dei sindaci con i cittadini arrabbiati. Dobbiamo evitare che la burocrazia distrugga le buone cose che si sono fatte, ovvero che lo Stato possa intervenire laddove l'infrastruttura non c'è. Questo è avvenuto negli anni 50 e 60 con le strade, con la rete elettrica; oggi dobbiamo superare ulteriormente le sperequazioni territoriali.
La prima sperequazione - credo che nessuno metta in dubbio – è che 5 milioni di italiani non vedono correttamente i primi canali Rai, può sembrare strano ma i ripetitori nelle aree montane del paese - 54% d'Italia - sono gestiti dagli Enti locali, e con i passaggi al digitale terrestre tutto si è complicato. La nuova tecnologia non ci ha aiutato. Ha generato sperequazioni. Questo è un tema che molto spesso nei Palazzi non entra e dobbiamo invece farlo entrare perché fa parte di quei diritti di cittadinanza, fa parte di quella necessità di coesione che il paese ha.
Sperequazioni che rischiano di aumentare anche con l'introduzione del 5G. Nel piccolo mondo antico non ci voglio stare, nel piccolo mondo antico invece rimaniamo se non creiamo consapevolezza che su queste sfide si riesce a guardare al futuro.

Uncem è nata nel 1952, per dare corpo e forza alle istanze dei territori montani italiani. Nasceva nel dopoguerra, quando sui territori sorgevano i primi "Consigli di Valle", là dove era nata la Resistenza e dunque, come scrive Calamandrei e ripete spesso il Presidente Mattarella, la Costituzione. Uncem subito ha riunito 3000 Comuni montani italiani, che dal 1973 hanno dato vita a una delle forme più evoluto di lavoro insieme, le Comunità montane. Uncem è "sindacato di territorio", ma anche "istituzione delle comunità". Lavora con la politica e con il sistema economico, con il terzo settore e tutta la PA, per guidare processi di sviluppo e crescita di territori complessi, zone che hanno opportunità che devono essere valorizzate con investimenti e apposite leggi. Uncem, con la vocazione statutaria a unire Comuni ed Enti

montani, prova a evitare frammentazione, lontananza dello Stato dalla montagna, soppressione dei diritti di cittadinanza. A partire da scuola, trasporti e sanità. Che sui territori ci sono sempre meno. E che inducono spopolamento e desertificazione delle Alpi e degli Appennini. Laddove la crisi climatica unita alla crisi demografica impongono soluzioni e progettualità di lungo periodo. Che includono anche digitalizzazione intrecciata a transizione ecologica ed energetica.
Uncem nasce per includere, creare reti, generare coesione. Così è stato nel 2008 quando sono nate, embrione subito cresciuto, le Green Community. Non un progetto, non un piano, ma una Strategia. Partita da quattro aree del sud Italia unendo Comuni, Comunità Montane, Enti parco, progettisti, in sinergia con Dipartimenti dei Ministeri e Regioni. Il punto è stato subito chiaro ed è fermo anche oggi: lavorare, Comuni insieme, su ambiti diversi vedendoli tutti connessi. Se intervengo sull'agricoltura, avrò ripercussioni anche sul turismo. E così sulle rinnovabili e sull'efficienza energetica, o il ciclo delle acque con quello dei rifiuti. E pure sul digitale. I Comuni per tradizione sono abituati a lavorare da soli e su ambiti specifici, quando hanno qualche finanziamento lo spendono. La Strategia delle Green Communities travolge questo meccanismo: si lavora insieme tra Enti, a livello di valle alpina e appenninica. Quanto si genera e realizza è figlio di una strategia. Altro punto chiave, si coinvolge la comunità. I cittadini, le imprese, le scuole, le associazioni. Tutti sono protagonisti del cambiamento e di un percorso che affronta la crisi climatica ed energetica senza lasciare alcuno indietro. È una rivoluzione nelle politiche pubbliche, che deve toccare tutti. Coinvolti e protagonisti. Se manca qualcosa, se i Comuni non lavorano insieme, se le membra non sono in relazione tra loro, la Strategia è monca. Vogliamo rendere oggi le Strategie d'area, quaranta, finanziate dal PNRR con 135 milioni di euro, realmente comunitarie.

Molto c'entra con la digitalizzazione della PA, degli Enti locali. Non si possono affrontare crisi ecologica, crisi energetica, crisi demografica – con le Strategie territoriali delle Green Community o delle Aree interne, ad esempio – se non connettiamo tra loro sedi, luoghi, spazi, uffici dei nostri Comuni. Oggi sono tutti frammentati, avranno anche il miglior gestionale di sempre, ottenuto con i voucher del PNRR certo, ma poi tra loro i Comuni non sono in dialogo. E allora tutto diventa vano, anche PAGOPA o SPID usato dal 99% dei cittadini per entrare in contatto con il Comune. Come stiamo insieme passa da una rinnovata sinergia tra sistemi territoriali, dunque tra le forme organizzate della democrazia sui territori. Su questo abbiamo moltissimo da fare. Percorsi e scenari non sempre chiari ed efficaci, visioni ancora da inquadrare, urgenze di Paese che non sempre coglie cosa sono i paesi. Nella legge 158 del 2017 sui piccoli Comuni vi era un chiaro riferimento al lavoro insieme, verso forme di "e-government" sovracomunali. Ci siamo arrivati in minima parte.

La logica comunitaria non è dei Comuni. In sostanza, tutti gli Enti sono ancora municipalisti e campanilisti. Più di alcuni anni fa. Anche sul fronte della digitalizzazione è così. La tradizione ad agire insieme c'è oggi, non ovunque, ma c'era forse

vent'anni fa più di oggi. Mi riferisco al drammatico abbattimento in diverse regioni italiane delle Comunità montane. Senza nostalgia o passatismo. Qui si, in questi enti, prevaleva una logica comunitaria nell'impostare progetti e strategie. Anche sull'"informatizzazione" dei Comuni non si sono fatti passi in avanti. C'erano soluzioni importanti già vent'anni fa. Non da soli, i Comuni. Lavorare insieme non è semplice, coinvolgere le comunità ancor più difficile. Le Comunità montane sono state distrutte sulla scorta di ideologie dannose per la montagna. Si è ripartiti, con molta fatica, in diverse regioni, con le Unioni montane di Comuni. Ma qui, oggi, deve entrare in gioco lo Stato centrale, con le regioni, nel favorire processi di associazionismo tra Comuni che poi possono contagiare le comunità. Questo processo si impara, è tra i compiti di un sindaco. Che vanno formati e informati rispetto all'importanza di queste urgenze che sono determinanti per i Comuni stessi. Fare quello che si faceva fino a ieri, non serve più. Cambiare paradigma vuol dire ripensare totalmente i Comuni, le forme aggregative, il ruolo del Sindaco. Ecco perché Uncem ha proposto recentemente un dibattito "sinodale" su come si cammina insieme e cosa si fa per essere in sinergia, ecosistemi che approntano un umanesimo nuovo capace di trasformare le istituzioni pubbliche.

La domanda è chiara. Come il processo di digitalizzazione può favorire innovativi modelli economici e dell'agire sociale all'interno delle Green Communities? Una sfida epocale, viste le enormi risorse economiche in ballo in questa fase, grazie al PNRR e alle programmazioni comunitarie. E vista anche la rivoluzione dei processi che la pandemia ha portato. E ancora: ma gli Enti locali in tutto questo? I Comuni delle periferie geografiche? Servono tanta formazione e supporto che insista su un punto centrale: da soli, per la digitalizzazione e la transizione tecnologica, da soli si può fare nulla. Spendere i voucher, ad esempio, previsti dal PNRR, a livello municipale, è (stato) assurdo. Purtroppo il Piano di ripresa e resilienza ha agito in questo senso. E ora occorre ricomporre. Questo Paese non regge più 34 mila centri di costo pubblici. E 7900 Comuni italiani, su digitale e rivoluzione ecologica in particolare, devono agire insieme. Grandi e piccoli Enti. Vuol dire che il cloud e i sistemi informativi sono condivisi, agevolano il lavoro insieme. Da qui si parte a lavorare su Intelligenza artificiale, blockchain, metaverso. Tre fronti sui quali siamo all'anno zero. Ma anche questi processi, devono essere orientati a generare coesione tra le comunità e tra gli Enti. È un processo nuovo. Le Green Communities sono anche questo. Capacità di andare oltre i confini. E il digitale ci aiuta, in questo e non solo.

Senza comunità, i Comuni non esistono. Solo due lettere in più nel primo sostantivo, che fanno la differenza per il secondo. Ma ancora non lo capiamo. Un patto tra i cittadini è quello che genera comunità e che rende vivo il Comune, piccolo o grande che sia. Nei piccoli centri, nei paesi, è più semplice rispetto alle città, a molti quartieri urbani, condividere tempo, idee, fatiche, impegno. La comunità si plasma (s)e i cittadini si sentono parte di un disegno. Nelle zone montane questo impegno vuol dire affrontare con modalità nuove le crisi climatica e demografica intrecciate e

interdipendenti. Ma c'è poi un altro termine decisivo. Territorio. Come la comunità sta sul territorio. Come genera inclusione, come esce dai confini comunali (dal territorio che è comfort-zone) e scegliere di essere protagonista in un'area geografica omogenea che nella storia è quasi sempre stata "aperta", ovvero capace di includere e di scegliere di non perdersi nelle debolezze orografiche. Un patto anche con le aree urbane, che la montagna innesta per il futuro. Perché l'interdipendenza è decisiva. La crisi ecologica ripropone le aree montane quale nuovo spazio dove abitare e lavorare con condizioni molto diverse dalle anguste aree urbane. Lavoriamo su questo. Comunità che, come scrive la Carta europea, si muovono nella digitalizzazione, nelle trasformazioni, in quei "fattori abilitanti" i nuovi servizi che hanno bisogno di governance locale, di istituzioni in dialogo, di Politica. Attivando leve istituzionali e investimenti, infrastrutture e servizi. La comunità fa la differenza.

N. 3 - 2025 - pp. 21-39

# Governance algoritmica dei principi digitali europei: modelli e prospettive

**Massimo Farina**

**Abstract**: La Dichiarazione europea sui Diritti e i Principi Digitali per il Decennio Digitale rappresenta un tentativo ambizioso di guidare la trasformazione tecnologica dell'Unione Europea secondo valori condivisi come centralità della persona, inclusione, libertà di scelta, partecipazione democratica, sicurezza e sostenibilità. Questo contributo analizza il ruolo delle Regulatory Technologies (RegTech) e delle Supervisory Technologies (SupTech) come strumenti abilitanti per la concreta attuazione di tali principi all'interno degli ecosistemi digitali. Attraverso un percorso che intreccia riflessione teorica, analisi normativa e osservazione di casi applicativi, il saggio mostra come le RegTech e SupTech possano trasformare la regolazione in un processo continuo, adattivo e verificabile, capace di coniugare automazione e controllo umano. L'obiettivo è evidenziare le potenzialità e i limiti di queste tecnologie nel contribuire a una governance digitale che sia al tempo stesso efficace, trasparente e rispettosa dei diritti fondamentali. In conclusione, si propone una visione evolutiva della Dichiarazione come base per una futura costituzionalizzazione del digitale in chiave europea, fondata su interoperabilità, responsabilità condivisa e apertura degli standard.

The European Declaration on Digital Rights and Principles for the Digital Decade sets out an ambitious vision to steer the European Union's technological transformation in line with shared values such as human-centredness, inclusion, freedom of choice, democratic participation, security, and sustainability. This paper explores the potential of Regulatory Technologies (RegTech) and Supervisory Technologies (SupTech) as enabling tools for the practical implementation of these principles within digital ecosystems. Through a path that interweaves theoretical reflection, regulatory analysis and observation of application cases, the essay shows how RegTech and SupTech can transform regulation into a continuous, adaptive and verifiable process, capable of combining automation and human control. The aim is to highlight both the opportunities and the critical challenges these technologies pose in promoting a digital governance model that is effective, transparent, and respectful of fundamental rights. The paper concludes by framing the Declaration as a foundational step towards a European model of digital constitutionalism, grounded in interoperability, shared accountability, and open standards.

**Parole chiave:** Digital Constitutionalism – Regulatory Technologies (RegTech) – Supervisory Technologies (SupTech) – Fundamental Rights – Human-Centred AI Governance



# 1. Introduzione

La Dichiarazione europea sui Diritti e i Principi Digitali per il Decennio Digitale (nel prosieguo semplicemente Dichiarazione o Carta) – adottata il 15 dicembre 2022 dalle tre istituzioni dell'Unione e pubblicata il 23 gennaio 2023[1] – costituisce il tentativo più compiuto di fondare la costituzionalità del digitale entro lo spazio giuridico europeo. Pur privo di efficacia vincolante, questo documento istituzionale sta al vertice di una piramide dinamica di strumenti di *soft law* – dalla Bussola Digitale 2030[2] (meglio nota come *Digital Compass* 2030) alle Comunicazioni COM (2022) 27[3] e 28[4] – articolandosi in dodici considerando e sei capitoli, che reinterpretano in chiave tecnologica i principi di libertà, eguaglianza e solidarietà, estendendoli ai temi della resilienza, della partecipazione e della sostenibilità. Come è stato puntualmente osservato[5], la Dichiarazione ha una natura programmatica ed esortativa, quindi priva di meccanismi di *enforcement* e di diritti immediatamente azionabili. Questa carenza di cogenza rischia di ridurla a un semplice manifesto politico, a meno che non si adottino strumenti in grado di tradurne i principi in obblighi operativi verificabili. Il vuoto è colmato dall'ecosistema *RegTech/SupTech* proposto in questo saggio,

[1] Dichiarazioni Comuni, Parlamento Europeo, Consiglio e Commissione Europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale,* 2023/C 23/01, 23 gennaio 2023.

[2] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni. Bussola per il digitale 2030: il modello europeo per il decennio digitale, (COM (2021) 118 final), 9 marzo 2021. La *Digital Compass* 2030 è, in sintesi, una comunicazione strategica adottata dalla Commissione Europea, che definisce gli obiettivi digitali dell'UE da raggiungere entro il 2030 e viene spesso descritta come un *framework* di orientamento per la trasformazione digitale dell'Europa. L'analogia simbolica con la bussola deriva dalla sua articolazione attorno a quattro aree cardinali, che costituiscono le direttrici strategiche della politica digitale europea: competenze digitali; infrastrutture digitali sicure e performanti; Trasformazione digitale delle imprese; digitalizzazione dei servizi pubblici.

[3] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali, (COM (2022) 27 final), 26 gennaio 2022.

[4] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, (COM (2022) 28 final), 26 gennaio 2022.

[5] L. Cianci, *Dichiarazione europea sui diritti e i principi digitali: quid pluris?*, in *Diritto pubblico comparato ed europeo*, 2, 2022, pp. 381-390.

che converte i valori dichiarati in *routine* di *compliance-by-design* costantemente monitorate. A spingere verso questa iniziativa sono tre tendenze concomitanti: l'"iperaccelerazione" delle innovazioni digitali (dall'IA generativa all'*edgecloud* ibrido fino alle reti 6G), che genera nuovi vuoti normativi; la "competizione strategica" con sistemi extraUE che adottano approcci diversi nell'equilibrio tra innovazione e diritti; e il crescente "*deficit* di fiducia" dei cittadini nei confronti di piattaforme *online* e istituzioni pubbliche.

Il cuore della Dichiarazione può essere identificato nella pretesa di far coesistere innovazione e garanzia in un'architettura regolatoria multilivello, laddove all'Unione spettano le regole di cornice (AI Act, DSA, DMA, DGA, EHDS)[6] e gli obiettivi misurabili (*Digital targets* 2030[7]), mentre gli Stati membri curano l'armonizzazione interna e gli attori privati l'implementazione responsabile. Nonostante la ricchezza di disposizioni *hardlaw*, l'esperienza recente del GDPR[8] ha mostrato che senza soluzioni operative *by design* i princìpi restano lettera morta[9]. Da qui l'interesse per gli artefatti tecnici che incorporano la regola nel codice, riducendo la distanza temporale tra innovazione e tutela[10] e lo stimolo per una riflessione sulle *Regulatory Technologies* (*RegTech*) e le *Supervisory Technologies* (*SupTech*) come dispositivi chiave per

---

6 "AI Act": Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828; "DSA": Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE; "DMA": Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati contendibili ed equi nel settore digitale e che modifica le direttive 2019/1937 e 2020/1828; "DGA": Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, sulla governance europea dei dati e che modifica il regolamento (UE) 2018/1724; "EHDS": Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, relativo allo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

7 Per il quadro completo dei *target* digitali per il 2030 e le modalità di attuazione, si veda *Europe's Digital Decade: digital targets for 2030*, disponibile all'indirizzo: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

8 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

9 R. Baldwin, M. Cave, *Understanding Regulation: Theory, Strategy and Practice*, 2ª ed., Oxford, 2012.

10 In un contesto di rapida innovazione tecnologica, gli "artefatti tecnici" (ossia di componenti *software* – come *smart contract*, motori di "*compliance by design*" e moduli di *audit* automatico – che traducono le disposizioni normative in regole immediatamente eseguibili da un sistema informatico) potrebbero essere efficaci strumenti per ridurre drasticamente il divario temporale (*regulatory lag*) tra la formulazione di nuove norme e la loro effettiva applicazione, assicurando una tutela dei diritti tempestiva ed efficace. Cfr.: H. Surden, *Machine Learning and Law*, in *Washington Law Review*, 89(1), 2014, pp. 87-115; D.W. Arner, J. Barberis, R.P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, in *Northwestern J. of International Law & Business*, 37(3), 2017, pp. 371-413.

"mettere in funzione" la Dichiarazione[11]. Nel contesto che qui si vuole richiamare *RegTech* indica il complesso di strumenti che convertono prescrizioni giuridiche in *routine software* eseguibili: motori semantici che estraggono obblighi da testi normativi, *smart contract* che automatizzano clausole di consenso, *ledger blockchain* che attestano immutabilità; *SupTech*, invece, designa l'insieme di piattaforme analitiche che potenziano le Autorità di vigilanza attraverso i *big data* e l'Intelligenza Artificiale: *dashboard* di *risk scoring*, modelli predittivi per l'*insider trading*, nonchè sistemi di *continuous audit*.

La domanda che muove l'indagine è duplice. Da un lato, ci si chiede, come far sì che i valori della Carta – centralità della persona, solidarietà, libertà di scelta, partecipazione, sicurezza, sostenibilità – diventino *default settings* dell'ecosistema digitale europeo; dall'altro, quali limiti epistemici ed eticopolitici emergono quando si passa dalla disposizione testuale alla norma computabile. La più efficace risposta può scaturire da un metodo trifasico che consta di analisi ermeneutica (rilettura della Dichiarazione con le lenti della filosofia del diritto), *mapping* regolatorio (ricomposizione dell'attuale *patchwork* UE in materia di dati, IA, mercati, salute, cybersicurezza) e analisi di *case studies* (verifica empirica di soluzioni *RegTech* – pseudonudonimizzazione automatica, *privacyenhancing technologies* – e *SupTech* – *dashboards* di monitoraggio in tempo reale e modelli di *anomaly detection*) alla luce dei sei capitoli della Carta.

Individuato, così, il tema di indagine all'interno di una cornice macroistituzionale, con opportuna manifestazione della necessità di un "travaso" continuo di valori in codice, si proseguirà il percorso attraverso l'articolazione teoricoconcettuale delle categorie *RegTech* e *SupTech* e la modellizzazione del diritto come macchina eseguibile, premessa indispensabile per l'analisi applicativa dei successivi paragrafi tematici.

# 2. Inquadramento teorico e concettuale

La premessa del paragrafo introduttivo – ossia, l'inderogabile esigenza di garantire che i valori e i principi sanciti dalla Carta europea dei diritti fondamentali trovino effettiva applicazione non solo nel diritto formale, ma anche all'interno dei codici e delle piattaforme che strutturano e regolano crescentemente la nostra vita quotidiana – impone una profonda e necessaria ridefinizione del rapporto tra norma

[11] D.W. Arner, J. Barberis, R.P. Buckley, *op. cit.*. L'articolo è di notevole utilità le sue definizioni e discussioni iniziali sulle *RegTech* e *SupTech* nel più ampio contesto dell'innovazione tecnologica applicata alla regolamentazione e alla vigilanza.

giuridica e regola tecnica[12]. Non si tratta più, infatti, di limitarsi a sovrapporre nuove regole o divieti a tecnologie preesistenti e già sviluppate, ma piuttosto di abbracciare la prospettiva secondo cui le tecnologie stesse e la loro intrinseca architettura divengono parte costitutiva dell'ordinamento giuridico e strumenti di *governance*. Poiché la Dichiarazione si presenta priva di valore normativo *stricto sensu*[13], le *RegTech* e le *SupTech* assumono la funzione di *hard-enforcement* tecnologico: incorporando gli obblighi direttamente nelle infrastrutture digitali trasformano l'enunciato programmatico in controlli automatici, auditabili e continuamente aggiornabili, assorbendo l'inattuabilità tipica della *soft law* nella prassi operativa[14]. In questa prospettiva, emerge con forza la centrale intuizione della *machine readable law*[15], ossia l'idea che la disposizione, per essere pienamente efficace e per agire proattivamente in un ambiente digitale, debba potersi trasformare in istruzioni che i sistemi *software* sono in grado di interpretare ed eseguire autonomamente, senza la necessità di attendere il giudizio *ex post* di un'autorità o di un tribunale[16].

La trasformazione della regola giuridica in codice eseguibile e in protocolli *embedded* si traduce in una duplice, significativa conseguenza che incide profondamente sul modo in cui la regolazione opera nel contesto digitale. Da un lato, assistiamo a una compressione della temporalità del controllo normativo e ciò accade perché, data la natura stessa degli atti digitali che si compiono in tempo reale, la verifica di conformità o l'applicazione della regola tende sempre più ad avvenire nel medesimo istante in cui l'azione ha luogo, riducendo drasticamente quello sfasamento temporale che tradizionalmente esisteva tra l'emergere di nuove pratiche e la successiva risposta del diritto. Parallelamente, sul piano materiale, si verifica una profonda mutazione nella natura stessa della regola, in quanto accanto alle tradizionali e ben note fonti del diritto – come i codici normativi e le sentenze dei tribunali – assistiamo all'emergere e all'assunzione di un peso sempre maggiore da parte di *standard* tecnici, linee guida operative e protocolli di settore. Sono elementi che spesso vengono incorporati direttamente nel codice sorgente, che non si riducono a semplici indicazioni operative ma funzionano di fatto come una vera e propria costituzione invisibile del *cyberspazio*[17], determinando in modo concreto e vincolante le possibilità d'azione e le interazioni all'interno dello spazio digitale, talvolta anche

---

[12] Su questa ridefinizione del rapporto tra diritto e tecnologia, e sulla concezione della tecnologia come parte dell'ordinamento giuridico (la "*rule of code*"), si veda P. De Filippi, A. Wright, *Blockchain and the Law: The Rule of Code*, Cambridge, 2018.

[13] A. Barbera, *La Carta europea dei diritti: una fonte di ri-cognizione?*, in *Il diritto dell'Unione Europea*, 6(2-3), 2001, 241-259.

[14] E. Mostacci, *La soft law nel sistema delle fonti: uno studio comparato*, Padova, 2008.

[15] Il concetto di *machine readable law* e la sua implicazione sulla necessità di tradurre le norme in istruzioni eseguibili dal *software* sono centrali nell'analisi di P. De Filippi e A. Wright, *op. cit.*

[16] H. Surden, *op. cit.*.

[17] J. Black, *Decentring Regulation: Understanding the Role of Regulation and Self Regulation in a "Post Regulatory" World*, in *Current Legal Problems*, 54, 2001, pp. 103 146.

prima o indipendentemente dalle norme giuridiche formali.

All'interno di questa cornice prendono forma le *Regulatory Technologies* e le *Supervisory Technologies*. Con la prima espressione ci si riferisce alla strumentazione con cui imprese, Pubbliche Amministrazioni e sviluppatori traducono obblighi e divieti in procedure automatiche[18], mentre con la seconda si indicano i dispositivi attraverso i quali le Autorità di vigilanza sorvegliano in modo continuo e proattivo l'osservanza delle regole[19]. Entrambe derivano da un principio comune – *compliance by design* – che la Dichiarazione rende esplicito soprattutto nei capitoli dedicati alla centralità della persona e alla sicurezza, per cui la conformità non deve essere un'operazione esterna al ciclo di sviluppo, ma un attributo nativo dei sistemi informativi.

La richiamata trasformazione non è neutrale[20], di conseguenza, se la norma diventa algoritmo, occorre preservare la trasparenza delle logiche decisionali, la ricostruibilità delle catene causali e la reversibilità delle scelte automatizzate[21]. Qui la dottrina della metaregolazione[22] offre una chiave interpretativa preziosa in base alla quale l'ordinamento giuridico può chiedere ai soggetti regolati di costruire in pro-

---

[18] Esempi tipici sono i motori semantici che estraggono obblighi da testi normativi, i "*terms of service scanner*" che segnalano clausole abusive e gli *smart contract* impiegati nei servizi di pagamento digitale.

[19] Le piattaforme *SupTech* oggi in uso presso ESMA (*European Securities and Markets Authority*) ed EBA (*European Banking Authority*) integrano modelli di *anomaly detection* e strumenti di *data visualisation* per il monitoraggio *real time* dei mercati finanziari.

[20] Per una critica approfondita della presunta neutralità della tecnologia e degli algoritmi, e per un'analisi dei rischi di *bias* e opacità ("scatole nere"), si veda F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2015.

[21] La necessità di garantire trasparenza, ricostruibilità (spiegabilità/auditabilità) e possibilità di sindacato/reversibilità delle decisioni automatizzate, specialmente in contesti con impatto sugli individui, è ampiamente dibattuta. Cfr. D.K. Citron, F. Pasquale, *The Scored Society: Due Process for Automated Predictions*, in *Washington Law Review*, 89(1), 2019, pp. 1-33; B. Goodman, S. Flaxman, *European Union regulations on algorithmic decision-making and a "right to explanation"*, in *AI Magazine*, 38(3), 2017, pp. 50-57.

[22] La meta-regolazione si caratterizza per il trasferimento, ai soggetti regolati, del compito di definire e implementare internamente i meccanismi di controllo necessari a rispettare obiettivi normativi stabiliti dall'autorità. Tali meccanismi – che possono includere *policy* interne, sistemi automatizzati di verifica e *report* di conformità – devono però essere progettati per essere auditabili dall'esterno, ovvero soggetti a ispezione e valutazione indipendente da parte di enti regolatori o organismi terzi. Questo paradigma, noto anche come "regolazione dei sistemi di regolazione", unisce la flessibilità dell'autoregolamentazione alle garanzie di trasparenza proprie della regolazione tradizionale. Cfr. C. Parker, *The Open Corporation: Effective Self Regulation and Democracy*, Cambridge, 2002. Nel contesto italiano, la meta-regolazione è stata oggetto di approfondimento soprattutto in ambito dottrinale penalistico e di *governance* digitale. Tra i contributi più rilevanti si ricordano: F. Venturi, *Per una balistica regolatoria dell'autonormazione in materia penale. Analisi descrittiva e prescrittiva del sistema di responsabilità ex crimine degli enti nell'orizzonte del post-regulatory state*, in *Criminalia*, 2021, pp. 161-208; L. Ammannati, *Regolatori e supervisori nell'era digitale: ripensare la regolazione*, in *Giurisprudenza Costituzionale*, LXVIII, fasc. 3, 2023, pp. 1453-1473. E. Bindi, E. Cremona, *La regolazione delle grandi piattaforme digitali*, in *Ianus - Diritto e Finanza*, n. 27, 2023, pp. 85-96.

prio i meccanismi di controllo, purché tali meccanismi siano auditabili[23] dall'esterno. Le *SupTech*, in questo scenario, divengono lo strumento che consente al regolatore di tenere in mano il filo del discorso, evitando che la delega degeneri in autoreferenzialità.

Il ricorso a *RegTech* e *SupTech*, tuttavia, solleva anche questioni di giustizia sostanziale. Gli algoritmi, infatti, sono inconsapevoli, per loro natura, dei limiti imposti dai diritti inderogabili e possono riprodurre i *bias* presenti nei dati di addestramento[24]. È quindi necessario integrare nel *design* degli strumenti tecnici meccanismi di controllo umano, linee guida etiche e protocolli di valutazione d'impatto. Sembra che l'AI Act si stia orientando con decisione in questa direzione, come testimonia l'imposizione di stringenti requisiti di supervisione umana (*human oversight*) per i sistemi considerati ad alto rischio. Tuttavia, è evidente che la sola volontà politica, pur necessaria, non è sufficiente a colmare il divario tra norma e implementazione tecnologica. Occorre, infatti, sviluppare e valorizzare professionalità intrinsecamente ibride, figure capaci di operare come ponte tra il mondo giuridico e quello informatico, traducendo efficacemente categorie e precetti del diritto in architetture software concrete ed eseguibili.

In questo scenario di crescente integrazione tra diritto e tecnologia, dove l'obiettivo è far vivere i valori fondamentali all'interno dei sistemi che regolano la nostra vita digitale e dove figure ibride come il *legal engineer* divengono cruciali

---

[23] In altri termini, il legislatore definisce obiettivi generali e parametri di *performance* (ad esempio livelli di sicurezza, protezione dei dati o *standard* di trasparenza), lasciando agli operatori la libertà di scegliere gli strumenti tecnici e organizzativi più idonei a conseguire tali risultati; la legittimità del sistema deriva allora non dalla rigida prescrizione di procedure, ma dalla verificabilità indipendente del loro funzionamento. Nel contesto delle *RegTech* e *SupTech*, la metaregolazione si traduce nell'adozione di *framework* che spingono gli sviluppatori di applicazioni digitali e gli operatori di vigilanza a imbastire internamente motori di *compliance* e *dashboard* di monitoraggio, purché apertamente sottoposti a esame da parte di *auditor*, enti supervisori o parti terze accreditate. Questo modello promuove l'innovazione, perché incentiva soluzioni personalizzate e flessibili, ma impone al contempo rigidi requisiti di trasparenza e responsabilità: qualsiasi modifica di un algoritmo sanzionatorio o di un meccanismo di segnalazione deve essere documentata e accessibile per ispezioni esterne, assicurando che la delega non si trasformi in una forma di autoregolamentazione opaca o autoreferenziale.

[24] Tra gli autori che hanno discusso esplicitamente i limiti degli algoritmi nel contesto della *legal automation* evidenziandone gli aspetti etici ed anche il pericolo di *bias* e la mancanza di sensibilità ai principi fondamentali, si vedano: M. Hildebrandt, *Smart Technologies and the End(s) of Law*, Cheltenham, 2015; C. Coglianese, D. Lehr, *Regulating by Robot: Administrative Decision Making in the MachineLearning Era*, in *Georgetown Law Journal*, 105(4), 2017, pp. 1147-1223; B.D. Mittelstadt, et al., *The Ethics of Algorithms: Mapping the debate*, in *Big Data & Society*, 3(2), 2016, pp. 1-21. In tema, si vedano anche G. Sartor, *L'intelligenza artificiale e il diritto*, Torino, 2022; U. Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, Berlino, 2013. Senza un richiamo esplicito alle tecniche algoritmiche, Luigi Ferrajoli, in L. Ferrajoli, *Diritti fondamentali: un dibattito teorico*, Bari, 2008, affronta i fondamenti della garanzia dei diritti e sottolinea la necessità di tutelare i diritti fondamentali contro derive autoritarie o arbitrarie. Traslato nell'attuale contesto tecnologico, il suo garantismo può essere minacciato dall'inconsapevolezza degli algoritmi.

per tradurre il diritto in codice eseguibile – una direzione peraltro già intrapresa da normative come l'AI Act con i suoi requisiti di *human oversight* per i sistemi ad alto rischio – un indispensabile orizzonte assiologico è offerto dai principi elaborati da pensatori che hanno profondamente indagato la natura del diritto e il suo rapporto con la società e la tecnologia. Essi forniscono le lenti concettuali necessarie per orientare questa profonda trasformazione e assicurare che il nuovo assetto ordinamentale sia pienamente compatibile con i valori fondamentali della Dichiarazione. Guardando all'enfasi posta sulla coerenza interna dell'ordinamento come fonte primaria della sua forza e validità, emerge anche il principio guida cruciale per cui le soluzioni basate su *RegTech* e *SupTech*, per essere legittime ed efficaci nel lungo periodo, devono saper dialogare e integrarsi armonicamente con l'intero sistema delle fonti del diritto, quindi non limitarsi a operare come frammenti tecnologici isolati o potenzialmente contraddittori rispetto al quadro normativo vigente[25]. Parallelamente, rivendicando il primato dell'autodeterminazione informativa e il controllo individuale sui dati personali, si impone la questione etica e giuridica tipica di ogni processo di automazione che impatti sulla sfera personale, ossia la necessaria previsione di meccanismi effettivi che lascino spazio alla libera revoca del consenso e alla portabilità dei dati[26]. L'idea di un diritto mite, fondato sul dialogo, sulla ponderazione e sulla proporzionalità anziché sulla mera imposizione punitiva, offre un ulteriore criterio fondamentale per valutare l'impatto degli algoritmi regolatori, sottolineando la necessità – proprio in virtù della loro capacità di operare in tempo reale e su larga scala – di modularne l'intervento in modo graduale, proporzionato e commisurato alle fattispecie[27]. Vi è, poi, il fattore ambientale complesso e interconnesso – e da custodire e preservare nel suo complesso – che implica responsabilità che vanno ben oltre la singola regola o il singolo dato. Applicato alle *RegTech* e *SupTech*, si traduce nel riconoscimento che la ricerca di efficienza, pur legittima, non deve avvenire a scapito della salvaguardia della pluralità delle voci, della qualità dei contenuti e della ricchezza complessiva dell'ecosistema digitale[28] in cui le tecnologie operano.

---

[25] Questo principio si rifà alla teoria dell'ordinamento giuridico, che enfatizza la coerenza interna e la sistematicità delle norme per la validità e l'efficacia del diritto. Si veda, ad esempio, N. Bobbio, *Teoria dell'ordinamento giuridico*, Torino, 1960. La sua pertinenza nel contesto di *RegTech* e *SupTech* risiede nella necessità che queste tecnologie si integrino armonicamente nel quadro normativo esistente.

[26] Sul diritto all'autodeterminazione informativa e sulla protezione dei dati personali, si veda, per tutti, S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014. Questo principio è cruciale per valutare l'impatto delle tecnologie che trattano dati personali ai fini regolatori o di vigilanza.

[27] Sul concetto di diritto mite, mediante il quale si vuole enfatizzare un approccio alla regolazione basato sulla proporzionalità, sul dialogo e sulla non eccessiva rigidità punitiva, contrapponendosi a un diritto inteso meramente come comando coercitivo, si veda G. Zagrebelsky, *Il diritto mite*, Torino, 1992. La sua rilevanza per gli algoritmi regolatori sta nella necessità di modulare l'intervento automatizzato in modo flessibile e graduale.

[28] È qui utile invocare il concetto di infosfera, caratterizzato da complessità e interconnessione di L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017. Applicato al paradigma *RegTech/SupTech*, invita a considerare l'impatto sistemico di queste tecnologie sull'intero ecosistema informativo e non solo sui singoli processi.

L'implementazione concreta delle *RegTech* e *SupTech*, sebbene guidata da questi principi filosofici, non è priva di sfide pratiche ed economiche che richiedono un'attenta considerazione. Gli studi di Baldwin e Cave[29] hanno evidenziato come le piattaforme *RegTech* possano condurre a significative riduzioni dei costi amministrativi per le imprese (stimate fino al 30%) ma hanno altresì sostenuto che una loro eventuale progettazione proprietaria rischierebbe di erigere nuove e insidiose barriere all'ingresso per i nuovi operatori. Ciò suggerisce una lettura del Capitolo V della Dichiarazione – relativo alla sicurezza e all'empowerment degli utenti e del mercato – orientata all'impegno concreto per l'adozione e la promozione di *standard* aperti e interoperabili, fondamentali per scongiurare situazioni di *lock-in* tecnologico e preservare la concorrenza. Similmente, le incoraggianti esperienze delle *SupTech* nel settore finanziario dimostrano un'accelerazione notevole nei tempi di segnalazione delle anomalie, passando da settimane a poche ore, un progresso notevole in termini di efficienza della vigilanza[30]. Questo avanzamento, parallelamente, amplifica il rischio di decisioni automatizzate che possono risultare opache o difficilmente comprensibili; da qui l'impellente esigenza, in linea con i principi di trasparenza e ricostruibilità già menzionati, di garantire spiegazioni chiare e accessibili riguardo al funzionamento e agli esiti di tali sistemi, anche a chi non possiede competenze tecniche avanzate.

In definitiva, l'inquadramento teorico qui proposto, che coniuga la necessità di tradurre valori in codice con i principi della filosofia del diritto e l'analisi delle implicazioni pratiche ed economiche delle nuove tecnologie regolatorie, svolge una duplice, essenziale funzione. Da un lato, esso chiarisce come le *RegTech* e le *SupTech* non siano meri strumenti tecnici, ma possano e debbano operare come vere e proprie cerniere – o *interfaces* – dinamiche tra l'impianto valoriale della Dichiarazione e le prassi concrete che si affermano nei mercati e negli spazi digitali; dall'altro, indica in modo puntuale e critico le cautele e le garanzie necessarie per assicurare che l'inevitabile ricerca di efficienza e automazione non avvenga a scapito dei principi democratici, dei diritti fondamentali e della contendibilità del potere digitale. Il passo successivo della presente analisi, e obiettivo dei paragrafi che seguiranno, consisterà pertanto nell'applicare sistematicamente questa griglia di lettura ai singoli capitoli della Carta, mostrando in che modo, principio per principio, i valori che essa incarna trovino (o, al contrario, rischino di non trovare) effettiva attuazione nelle tecnologie emergenti e nelle loro concrete modalità di impiego.

---

[29] Cfr. R. Baldwin, M. Cave, *op. cit.*

[30] Queste osservazioni si basano sulle prime esperienze e report sull'adozione delle *SupTech* nel settore finanziario e sulle loro implicazioni operative. Cfr. ad es. *report* della Banca dei Regolamenti Internazionali (BRI) o del *Financial Stability Board* (FSB) sull'argomento.

# 3. Analisi tematica secondo la Dichiarazione

La riconcettualizzazione della disposizione normativa come elemento eseguibile apre la strada per l'inquadramento delle *RegTech* e *SupTech* quali leve essenziali per la sua implementazione e, a questo scopo, impone preliminarmente di verificare come questi strumenti possano tradurre in prassi applicative i sei capitoli della Dichiarazione europea sui diritti e i principi digitali. Piuttosto che limitarsi a una mera corrispondenza terminepertermine, l'analisi che segue intende cogliere le tensioni, le potenzialità e i limiti insiti nel passaggio dai princìpi astratti a soluzioni tecnologiche concrete, ponendo in evidenza i collegamenti logici che rendono coerente l'intero approccio.

Il primo capitolo della Carta – *"Mettere le persone al centro della trasformazione digitale"* – sottolinea come le tecnologie debbano essere progettate partendo dai diritti e dalle esigenze degli individui. In questo contesto, le soluzioni *RegTech* potrebbero giocare un ruolo chiave nella traduzione dei principi di trasparenza e accessibilità in veri e propri elementi di interfaccia. Si pensi, ad esempio, ai motori semantici integrati, i quali potrebbero arricchire automaticamente i metadati delle applicazioni con informazioni sui diritti di ciascun utente, permettendo a sviluppatori e giuristi di verificare, già in fase di progettazione e sviluppo, la conformità dei flussi di dati alle aspettative normative[31]. Le soluzioni *SupTech*, invece, che mettono a disposizione delle autorità strumenti di controllo in tempo reale, possono essere impiegate per il monitoraggio della *user experience*, individuando tempestivamente anomalie nell'accesso dei cittadini ai servizi essenziali[32]. Poiché però l'effettiva inclusività dipende dalla rappresentatività dei *dataset*, eventuali sbilanciamenti possono tradursi in barriere d'uso non previste. Diventa quindi cruciale istituire un circuito di *feedback* continuo, in cui i dati e le segnalazioni emerse dalle *dashboards* di vigilanza vengano regolarmente riconsegnati al *team* di sviluppo, così da consentire – attraverso un approccio di *governance* riflessiva[33] – di correggere con rapidità eventuali lacune nell'esperienza digitale.

Proseguendo, il capitolo *"Solidarietà e inclusione"* sottolinea l'urgenza di colmare il divario digitale e di assicurare pari opportunità di accesso. Qui l'idea dell'impiego di *RegTech* emerge come abilitatore di controlli automatici di conformità agli

---

[31] Cfr.: D.W. Arner, J. Barberis, R.P. Buckley, *op. cit;* M. Ferraris, *Documentality. Why it is Necessary to Leave Traces*, New York, 2012.

[32] Cfr.: B. D. Mittelstadt, et al., *op. cit*; L. Grassi, *Cos'è il RegTech e come funziona: alcune caratteristiche*, 18 luglio 2024, articolo a cura dell'Osservatorio Fintech & Insurtech del Politecnico di Milano, consultabile all'indirizzo: https://blog.osservatori.net/it_it/cose-regtech-come-funziona-caratteristiche.

[33] N. Gunningham, P. Grabosky, D. Sinclair, *Smart Regulation. Designing Environmental Policy*, Oxford, 1998.

*standard* di accessibilità – dalle linee guida WCAG[34] alla localizzazione multilingue per comunità linguistiche di minoranza – integrando moduli che segnalano in anticipo potenziali barriere. In questa prospettiva trovano concreta applicazione i cosiddetti "diritti emergenti"[35] – fra cui il diritto alla disconnessione, la connettività universale e la tutela dell'eredità digitale – che la Dichiarazione porta alla ribalta. Soluzioni *RegTech* possono, ad esempio, implementare schedulatori che impongono pause obbligatorie nei sistemi di *remote working*, mentre *dashboard SupTech* monitorano in tempo reale il rispetto delle soglie di banda o l'esecuzione di *smart contract* destinati alla gestione *post-mortem* dei dati personali. Le *SupTech*, d'altro canto, potrebbero mettere a disposizione analisi geospaziali e modelli predittivi basati su *big data* per individuare i "deserti digitali" e le fasce di popolazione più vulnerabili. La logica regolatoria, per inciso, andrebbe, inoltre, completata con incentivi economici e meccanismi di solidarietà orizzontale, in quanto è chiaro che senza una compartecipazione finanziaria e senza strumenti di sanzione calibrata, persiste il rischio che l'inclusione rimanga un valore formale piuttosto che sostanziale.

Il terzo capitolo, dedicato alla "*Libertà di scelta*", sottolinea il diritto di ogni persona di scegliere liberamente servizi e tecnologie senza subire condizionamenti nascosti. In questo contesto, le soluzioni *RegTech* offrirebbero piattaforme di gestione del consenso estremamente dettagliate, che permetterebbero a ciascun utente di controllare puntualmente quali dati condividere e di revocare in qualsiasi momento tutte le autorizzazioni con un semplice *click*[36]. Parallelamente, gli strumenti *SupTech* monitorerebbero il mercato digitale alla ricerca di pratiche scorrette, come il *lockin*[37] e i *dark pattern*[38], consentendo alle autorità di individuare e interrompere tempestivamente comportamenti lesivi prima che diventino sistematici. Rimarrebbe tuttavia aperta la sfida di conciliare la necessità di trasparenza dei processi di vigilanza con la tutela dei segreti industriali. Affinché i supervisori possano esaminare i flussi di dati senza esporre algoritmi proprietari, sarebbe indispensabile definire API

---

[34] Le *Web Content Accessibility Guidelines* (WCAG) 2.1, pubblicate dal *World Wide Web Consortium* (W3C) nel 2018, definiscono principi, linee guida e *success criteria* per rendere i contenuti *web* percepibili, utilizzabili, comprensibili e robusti. Suddivise in quattro principi fondamentali (*perceivable*, *operable*, *understandable*, *robust*), forniscono un quadro di riferimento internazionale per garantire l'accessibilità digitale a persone con disabilità visive, uditive, motorie e cognitive: cfr. World Wide Web Consortium (W3C), *Web Content Accessibility Guidelines (WCAG) 2.1,* in *W3C Recommendation*, consultabili in: https://www.w3.org/TR/WCAG21/.

[35] L. Cianci, *op. cit.*

[36] Cfr.: D.W. Arner, J. Barberis, R.P. Buckley, *op. cit.*.; L. Grassi, *op. cit.*, dove si analizza il rapporto tra *RegTech* e *SupTech* e il ruolo delle piattaforme di "*consent as a service*" per la revoca granulare dei permessi.

[37] K. Yeung, *Algorithmic regulation: A critical interrogation*, in *Regulation & Governance*, 12(4), 2018, pp. 505-523.

[38] C.M. Gray, et al. *The Dark (Patterns) Side of UX Design*, in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI'18), Paper 534, 2018, pp. 1-14.

standardizzate[39] per lo scambio di informazioni e stabilire procedure di audit che garantiscano al contempo riservatezza e tutela della proprietà intellettuale.

Il quarto capitolo, *"Partecipazione allo spazio pubblico digitale"*, punta a coinvolgere i cittadini in spazi virtuali aperti, sicuri e affidabili per il dibattito pubblico[40], laddove le soluzioni di *RegTech* potrebbero integrare sistemi di *identity verification* basati su *smart contract*, capaci di certificare l'autenticità degli utenti preservando al contempo il loro anonimato quando necessario[41]. Analogamente, gli strumenti di *SupTech* potrebbero sfruttare algoritmi di *sentiment analysis* e *network analysis* per individuare in tempo reale tentativi di manipolazione di massa o campagne coordinate di disinformazione[42]. Un simile approccio richiederebbe però criteri di intervento degli algoritmi definiti con la massima trasparenza e soggetti a meccanismi di revisione giudiziaria[43], in modo da evitare derive di "censura digitale" e mantenere intatta la fiducia degli utenti[44].

*"Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità"* è la tematica del penultimo capitolo, ove si pone l'accento sulla necessità di un approccio proattivo alla sicurezza digitale, non più limitato alla reazione contro gli incidenti. Di grande utilità sarebbero le soluzioni *RegTech* volte ad integrare librerie di crittografia pre-certificata e moduli automatici per la segnalazione delle violazioni[45], mentre gli strumenti *SupTech* si baserebbero su modelli predittivi in grado di identificare potenziali attacchi informatici prima del loro manifestarsi[46], affiancando *continuous penetration testing* e *digital twin* delle infrastrutture critiche[47]. Il tema centrale qui riguarda la responsabilità. Sarebbe infatti essenziale, per evitare vuoti normativi in caso di errori o omissioni, definire con chiarezza i ruoli e gli obblighi del fornitore tecnologico, del gestore del servizio e dell'Autorità di regolazione, introducendo solidi meccanismi di *accountability* volti a garantire il diritto di riparazione degli utenti[48].

---

[39] In linea con in linea con le misure previste per i *gatekeeper* digitali. Cfr. Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati contendibili ed equi nel settore digitale e che modifica le direttive 2019/1937 e 2020/1828 (Digital Markets Act).

[40] Cfr. A. Chadwick, *The Hybrid Media System: Politics and Power*, Oxford, 2017.

[41] Cfr. D. W. Arner, J. Barberis & R. P. Buckley, *op. cit.*; P. De Filippi, A. Wright, *op. cit.*

[42] Cfr. S. Vosoughi, D. Roy, S. Aral, *The Spread of True and False News Online*, in *Science*, 359(6380), 2018, pp. 1146-1151.

[43] K. Yeung, *op. cit.*

[44] Cfr. L. Floridi, *The Logic of Information*, Oxford, 2019.

[45] Cfr. A. Cavoukian, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, 2010.

[46] Cfr. R. Sommer, V. Paxson, *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection*, in *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[47] Cfr. E. Negri, L. Fumagalli, M. Macchi, *A Review of the Roles of Digital Twin in CPSbased Production Systems*, in *Procedia Manufacturing*, 11, 2017, pp. 939-948.

[48] Cfr. L. Floridi, M. Taddeo, *What is data ethics?*, in *Philosophical Transactions of the Royal Society*,

Infine, invocando la "*Sostenibilità*", la Carta chiude, in prospettiva ecologica, volgendo lo sguardo verso l'impatto ambientale delle infrastrutture digital, che deve essere valutato e contenuto. L'impiego delle *RegTech,* in tale ultimo ambito, potrebbe integrare, fin dalla progettazione, le *dashboard* per il monitoraggio del *carbon footprint* dei *data center* e delle applicazioni, imponendo limiti di utilizzo nei periodi di picco energetico[49]. Parallelamente le *SupTech* aggregherebbero telemetrie energetiche per certificare la neutralità $CO_2$ dei servizi e individuare eventuali pratiche di *greenwashing*[50]. Per evitare che il perseguimento della sostenibilità si traduca in mero esercizio di facciata, ci si dovrebbe affidare a metriche indipendenti, aperte e accessibili a tutti gli *stakeholder*, garantendo così il rispetto del principio di trasparenza previsto anch'esso dalla Dichiarazione.

Da questo breve percorso analitico può evincersi chiaramente che le *RegTech* e le *SupTech*, quando implementate secondo criteri di rigore tecnico e sottoposte a forme di *governance* etica, hanno il potenziale di tradurre i principi strategici della Dichiarazione europea – quali centralità della persona, solidarietà, libertà di scelta, partecipazione, sicurezza e sostenibilità – in procedure operative efficaci. Tale traduzione non avviene però in modo automatico né privo di tensioni. L'innovazione tecnologica deve, infatti, confrontarsi con la salvaguardia dei diritti fondamentali e con l'esigenza di trasparenza delle logiche decisionali, richiedendo un bilanciamento dinamico tra automazione e supervisione umana, flessibilità progettuale e stabilità normativa.

Il prossimo paragrafo approfondirà tre casi studio europei reali, selezionati per la loro capacità di esemplificare sia i successi – in termini di efficienza, inclusività e responsabilità – sia le criticità operative – quali *bias* di sistema, problemi di interoperabilità e limiti di *accountability* – emerse in fase di implementazione. Queste esperienze offriranno preziosi spunti per perfezionare il modello di *governance* digitale delineato dalla Carta, evidenziando in che misura un approccio ibrido e partecipativo possa garantire non solo l'effettività delle soluzioni tecniche, ma anche la piena coerenza con i valori europei di giustizia sostanziale e trasparenza.

A374 (2083), 2016, pp. 1-5.

[49] Cfr.: A. Beloglazov, R. Buyya, *Energy Efficient Resource Management in Virtualized Cloud Data Centers*, in *Cluster Computing and the Grid, IEEE International Symposium*, Melbourne, 2010, pp. 826-831; J. Baliga, R. W. Ayre, K. Hinton, R. S. Tucker, *Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport*, in *Proceedings of the IEEE*, 99(1), 2011, pp. 149–167.

[50] Cfr. M. Hildebrandt, *op. cit.*; J. Malmodin, D. Lundén, *The Energy and Carbon Footprint of the Global ICT and E&M Sectors 2010–2015*, in *Sustainability*, 10(9):3027, 2018, pp. 1-31.

# 4. Casi di studio

A valle dell'inquadramento teorico – in cui si è vista la norma divenire flusso eseguibile tramite le *Regulatory Technology* e le *Supervisory Technology*[51] – e dell'analisi dei sei capitoli della Carta in chiave tecnologica, è giunto il momento di traslare il discorso dal piano delle idee e dei principi al piano degli esempi concreti. Attraverso la sintetica illustrazione di tre casi di studio, si cercherà di dimostrare come, in contesti reali e verificati, le tecnologie regolatorie e di supervisione traducano i valori della Dichiarazione europea in prassi operative, pur facendo emergere sfide strutturali che richiedono soluzioni di *governance* più raffinate.

Il primo caso è costituito dall'*eHealth Digital Service Infrastructure* (eHDSI) – noto anche come *MyHealth@EU* –, infrastruttura che garantisce lo scambio transfrontaliero di *Summary Patient Records* e di *ePrescriptions* tra gli Stati membri dell'Unione Europea. Fin dalla sua prima concezione, l'eHDSI integra smart contract e componenti *privacy by design*, applicando lo standard semantico FHIR XDS.b per pseudonimizzare i dati al momento dell'estrazione, in modo da rispettare i princìpi di "centralità della persona" e "libertà di scelta" della Dichiarazione. Il paziente mantiene il controllo sui propri consensi, la revoca o l'abilitazione all'accesso avviene comodamente tramite tessera sanitaria elettronica o *app*, realizzando pienamente la *compliance by design* senza interventi manuali. Sul fronte *SupTech*, i *National Contact Points for eHealth* trasmettono *log* di accesso a una *dashboard* centralizzata che applica algoritmi di *anomaly detection*, segnalando in tempo reale richieste ibride, transazioni fuori orario o accessi da indirizzi IP inconsueti. Questo meccanismo rispecchia il modello di *dynamic enforcement*[52] ed evita derive di automazione incontrollata, poiché ogni allarme è soggetto a una verifica umana secondo i principi

[51] Cfr. H. Surden, *op. cit.*.; C. Coglianese, D. Lehr, *op. cit.*

[52] L'espressione *dynamic enforcement* (applicazione o coercizione dinamica) si nutre di contributi provenienti da diverse discipline, tra cui il diritto, la scienza politica, la pubblica amministrazione, la sociologia e l'informatica. Sinteticamente, in chiave utile per questa sede, ci si riferisce all'applicazione della normativa che si discosta dai modelli tradizionali, statici e spesso basati su ispezioni periodiche o reattive. Si enfatizza l'uso proattivo e strategico di dati, tecnologie (come l'intelligenza artificiale e l'apprendimento automatico per l'analisi dei rischi e l'individuazione di anomalie) e una maggiore flessibilità operativa. L'obiettivo è ottimizzare l'allocazione delle risorse di controllo, adattare le strategie di *enforcement* in tempo reale in base alle informazioni emergenti e al comportamento dei soggetti regolati, e migliorare l'efficacia complessiva della vigilanza. Nel contesto del testo, il monitoraggio automatizzato dei *log* di accesso con segnalazione di anomalie per una verifica umana incarna proprio questo principio di applicazione delle regole che si adatta dinamicamente ai *pattern* di attività. Si veda C. Coglianese, D. Lehr, *op. cit.* Oltre a Cary Coglianese, tra coloro che hanno toccato concetti strettamente correlati al *dynamic enforcement*, si vedano: J. Braithwaite, *Restorative Justice & Responsive Regulation*, Oxford , 2002; M.K. Sparrow, *The Regulatory Craft: Controlling Risks, Solving Problems, and Managing Compliance*, Washington DC, 2000; D.K. Citron, *Technological Due Process*, in *Washington University Law Review*, 85(6), 2008, pp. 1249-1313; F. Pasquale, *op. cit.*

di *reflexive regulation*[53]. L'esperienza ha mostrato disallineamenti nelle codifiche regionali dei metadati e difficoltà di localizzazione linguistica, confermando la necessità di standard aperti per garantire interoperabilità e ridurre i *bias* introdotti da traduzioni inconsistenti. Questi ostacoli tecnici e semantici hanno evidenziato come l'effettiva realizzazione dei diritti nello spazio digitale dipenda criticamente dall'architettura e dall'implementazione delle infrastrutture sottostanti, un tema che è stato di centrale importanza nella riflessione di Stefano Rodotà sull'impatto della tecnologia sulla persona e sul diritto nell'era digitale[54].

Il secondo caso riguarda FIU.NET, la rete europea delle *Financial Intelligence Units* istituita dalla Direttiva UE 2015/849[55] per lo scambio di *Suspicious Transaction Reports*. FIU.NET unisce 28 Autorità nazionali in un'unica piattaforma *SupTech*, dove modelli di *link analysis* e *machine learning* spiegabile emergono come strumenti per individuare con rapidità reti di riciclaggio transnazionali[56]. Quando un algoritmo

---

[53] La *reflexive regulation* (regolazione riflessiva) è un approccio teorico e pratico alla regolamentazione che mira a incoraggiare l'autoregolamentazione da parte degli Enti vigilati. Piuttosto che imporre norme prescrittive dettagliate (cosiddetto modello *command-and-control*), la regolazione riflessiva cerca di influenzare i processi decisionali interni delle organizzazioni, stimolandole a riflettere criticamente sulle proprie *performance*, sui rischi e sulla conformità agli obiettivi normativi generali. L'idea è quella di creare meccanismi (informativi, procedurali, partecipativi) che inducano i soggetti regolati a internalizzare gli scopi della regolamentazione e a sviluppare autonomamente soluzioni efficaci e contestualizzate. Autori come Gunningham, Grabosky e Sinclair (1998), nel loro lavoro sulla "*smart regulation*", hanno integrato i principi della regolazione riflessiva, sostenendo l'uso di una combinazione di strumenti regolatori che includono l'autoregolazione guidata e la co-regolazione, dove la verifica umana degli allarmi automatici, come descritto nel testo, può essere vista come un meccanismo che assicura che l'automazione non sostituisca la capacità riflessiva e la responsabilità. Si veda: N. Gunningham, P. Grabosky, D. Sinclair, *op. cit*. Questi autori discutono come la regolazione possa essere resa più efficace orchestrando una varietà di strumenti e attori, inclusi quelli che promuovono l'autocontrollo e la riflessività da parte dei regolati.

[54] Questi aspetti critici sull'implementazione pratica delle infrastrutture digitali evidenziano la necessità di *standard* aperti e l'impatto del *design* tecnico sull'effettiva realizzazione dei diritti e principi giuridici (come l'interoperabilità, l'inclusione e la riduzione dei *bias*), rientrano appieno nell'ambito della riflessione di Stefano Rodotà sull'intersezione tra tecnologia, diritto e società, e sulla cruciale importanza dell'architettura dei sistemi digitali per la tutela della persona nell'era digitale. Si vedano, tra le varie opere dell'autore, in particolare S. Rodotà, *Tecnopolitica. Le democrazie e le nuove tecnologie della comunicazione*, Roma-Bari, 2004; Id., *La vita e le regole. Tra diritto e non diritto*, Milano, 2018; Id., *Il mondo nella rete, op. cit*.

[55] Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica il regolamento (UE) n. 648/2012 del Parlamento europeo e del Consiglio e che abroga la direttiva 2005/60/CE del Parlamento europeo e del Consiglio e la direttiva 2006/70/CE della Commissione.

[56] Si veda, K. Yeung, *op. cit.* L'Autrice, studiosa di spicco a livello internazionale nel campo della regolamentazione algoritmica e della *governance* della tecnologia, ha esplorato come i sistemi basati su algoritmi e analisi dei dati vengano impiegati per regolare, monitorare e indirizzare le condotte, con implicazioni significative per il diritto e la società. Nell'Opera citata, analizza criticamente l'ascesa di queste nuove forme di regolazione (tra cui rientrano anche quelle utilizzate in FIU.NET per l'individuazione di reati finanziari). L'impiego di sistemi algoritmici, anche con caratteristiche di *explainability*, in contesti di vigilanza e applicazione della legge solleva questioni giuridiche e filosofiche fondamentali, quali la trasformazione della natura della norma giuridica mediata o

rileva dei *pattern* sospetti, attiva gli *alert* automatici e suggerisce filtri *RegTech* che bloccano provvisoriamente le transazioni, incarnando i princìpi di "*Partecipazione allo spazio pubblico digitale*" e di "*Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità*" contenuti nella Dichiarazione. Le FIU (*Financial Information Units*), grazie all'adozione di tecniche di *explainable AI*, possono comprendere i parametri sottostanti ai segnali e calibrare la propria risposta, realizzando un ciclo virtuoso tra automazione e giudizio umano. Tuttavia, l'assenza di interfacce API uniformi limita la capacità delle singole unità di estrarre e confrontare statistiche, creando asimmetrie informative e ostacolando la "*libertà di scelta*" delle Autorità federate. Appare, pertanto, evidente che anche in contesti di massima criticità, un'applicazione parziale del paradigma *RegTech/SupTech* renda urgente un intervento di *designbased regulation* per standardizzare le API e promuovere la condivisione collaborativa dei dati[57].

Il terzo esempio si situa nel campo della rendicontazione finanziaria e della sostenibilità, con il *European Single Electronic Format* (ESEF) obbligatorio per i bilanci iXBRL (*Inline eXtensible Business Reporting Language*)[58] delle società quotate, introdotto dalla Direttiva 2013/34/UE[59]. Questa infrastruttura *RegTech* di massa ha

implementata nel codice e l'impatto che ne consegue sull'esercizio del potere pubblico e sui concetti tradizionali di responsabilità e controllo. Tale riflessione è centrale nella dottrina giuridica, e in particolare nella filosofia del diritto e nell'informatica giuridica. Autori come Stefano Rodotà (cfr. ad es. S. Rodotà, *Tecnopolitica*, *op. cit.*; Id., *Il mondo nella rete*, *op. cit.*) hanno precorso questi temi, evidenziando come l'infrastruttura tecnologica e il codice algoritmico assumano una valenza politica e regolativa, influenzando direttamente la sfera dei diritti e delle libertà. Nel diritto pubblico, Andrea Simoncini e Erik Longo, tra gli altri, hanno contribuito al dibattito sui diritti fondamentali nell'era algoritmica e sulle decisioni automatizzate da parte delle autorità pubbliche: A. Simoncini, E. Longo, *Fundamental Rights and the Rule of Law in the Algorithmic Society*, in H.W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021, pp. 27-41; A. Simoncini, E. Longo, *Il linguaggio dell'Intelligenza Artificiale e la tutela costituzionale dei diritti*, in *Rivista Associazione Italiana dei Costituzionalisti (AIC)*, 2, 2023, pp. 1-39.

[57] Si vedano, B.J. Koops, R.E. Leenes, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law*, in *International Review of Law, Computers & Technology*, 28(2), 2014, pp. 159-171. Sebbene questo specifico contributo si concentri sulla previsione *privacy by design* nell'ambito della protezione dei dati, esso solleva questioni fondamentali sulla possibilità e i limiti di incorporare requisiti normativi direttamente nella progettazione e nell'architettura dei sistemi tecnologici. L'analisi è pertinente per sostenere l'argomentazione nel testo poiché evidenzia l'importanza critica del *design* tecnico (come la standardizzazione delle API) per facilitare il raggiungimento di obiettivi regolamentari (in questo caso, l'interoperabilità e la condivisione dei dati per il contrasto al riciclaggio), e contribuisce al più ampio dibattito sulla necessità di interventi mirati sulla progettazione tecnologica per supportare o attuare le finalità del diritto, un aspetto centrale del paradigma del *design based regulation*.

[58] Nello specifico Si tratta di una tecnologia che consente di incorporare dati XBRL (*eXtensible Business Reporting Language*) direttamente all'interno di un documento HTML (*HyperText Markup Language*, che è il linguaggio *standard* utilizzato per creare pagine *web* leggibili dagli esseri umani tramite un *browser*).

[59] Direttiva 2013/34/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento europeo e del Consiglio e abrogazione delle

reso *machinereadable* il *reporting* contabile, traducendo i princìpi di "T*rasparenza*" e "*Sostenibilità*", contenuti nella Dichiarazione, in controlli automatici di coerenza e completezza. Con l'entrata in vigore della *Corporate Sustainability Reporting Directive*[60] (CSRD), ESMA e numerose *Authority* nazionali hanno sviluppato moduli *SupTech* in grado di analizzare i dati iXBRL per identificare omissioni o discrepanze nei report ESG (*Environmental, Social, and Governance*), attivando *alert* e comparazioni interaziendali che obbligano le imprese a un *reporting* più rigoroso. Questa sinergia *RegTech/SupTech* realizza un monitoraggio continuo della sostenibilità ambientale e sociale, ma sottolinea anche tensioni tra l'efficienza di automatismi sempre più sofisticati e l'aumento del fabbisogno energetico computazionale, problematica richiamata dal capitolo VI della Dichiarazione. Diventa, quindi, essenziale l'integrazione di metriche *ethics by design*, come propone Floridi[61], per bilanciare precisione analitica ed efficienza energetica, evitando che l'innovazione normativa si traduca in *greenwashing* o in nuove barriere tecniche per le PMI[62].

## 5. Verso il *digital constitutionalism* europeo

Dal percorso fin qui compiuto, emerge un paradigma di *governance* digitale ibrida, in cui la distinzione tra le *RegTech* e *SupTech* diventa sempre più sfumata. Mentre le prime forniscono protocolli eseguibili e le seconde li sorvegliano e li verificano, entrambe si trovano ad operare entro un ecosistema di norme, istituzioni e cittadinanza attiva. Senza un coordinamento multilivello e senza la partecipazione

direttive 78/660/CEE e 83/349/CEE del Consiglio.

[60] Direttiva (UE) 2022/2464 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che modifica il regolamento (UE) n. 537/2014, la direttiva 2004/109/CE, la direttiva 2006/43/CE e la direttiva 2013/34/UE per quanto riguarda la rendicontazione societaria di sostenibilità.

[61] Si rimanda, principalmente ma non esclusivamente, a L. Floridi, *L'etica dell'Intelligenza Artificiale. Sviluppi, opportunità, sfide*, Milano, 2020. Il concetto di *ethics by design*, promosso dall'Autore e discusso in diverse sedi, sottolinea l'importanza cruciale di incorporare considerazioni etiche fin dalle prime fasi della progettazione e dello sviluppo dei sistemi di IA e delle tecnologie digitali. Il richiamo al pensiero di Floridi si rivela particolarmente efficace per rafforzare l'argomentazione sulla necessità di bilanciare gli aspetti tecnici (precisione, efficienza computazionale) con valori etici (come la sostenibilità e l'inclusività, evitando il *greenwashing* e le barriere per le PMI), promuovendo tale bilanciamento come impostazione predefinita (*by default*).

[62] Si veda, M. Hildebrandt, *op. cit.*. L'illustre giurista nell'ambito del diritto e delle tecnologie emergenti analizza come le tecnologie intelligenti (tra cui rientrano gli automatismi sofisticati e l'IA impiegati nelle *SupTech/RegTech*) stiano riconfigurando il diritto e la società. La sua opera esplora le implicazioni profonde dell'uso pervasivo di tecnologie basate sull'analisi dei dati e sull'apprendimento automatico, evidenziando le sfide che si pongono per il diritto. Il pensiero dell'Autrice fornisce una base teorica per comprendere le tensioni e le nuove problematiche (come l'aumento del fabbisogno energetico computazionale o la creazione di barriere tecniche) che emergono dall'applicazione di tecnologie sofisticate in ambiti regolamentati, sostenendo indirettamente l'urgenza di un approccio normativo che consideri attentamente gli impatti di tali tecnologie.

strutturata dei portatori di interesse – cittadini, imprese, autorità di regolazione – si rischia di trasformare l'automazione in tecnocrazia e il monitoraggio in sorveglianza generalizzata. Per evitare tale deriva, la Carta digitale europea dovrebbe evolversi in un vero *digital constitutionalism*[63], in cui principi di trasparenza, responsabilità e consultazione pubblica non siano meri *slogan*, ma obblighi integrati nelle architetture dei sistemi. In questo quadro, le *RegTech* e le *SupTech* potrebbero configurarsi come architetture di bilanciamento dinamico, che incorporano garanzie procedurali – *explainability*, *algorithmic impact assessments*, *audit* indipendenti e *meaningful human oversight* – traducendo così i princìpi costituzionali in prassi tecniche verificabili.

In prospettiva, l'elaborazione di un modello coerente multilivello – in cui le Carte globali, l'ordinamento UE, le costituzioni nazionali e persino i *terms of service* aziendali possono federarsi – richiederebbe l'adozione di *standard* aperti e di un'unica *grammar* semantica per i dati sanitari, finanziari e contabili; l'istituzione di un Centro europeo per la *governance* digitale che supporti Stati membri e Autorità con linee guida tecniche aggiornate e servizi di *testing* interoperabile; la definizione di metriche condivise per la misurazione dei *bias* e dell'impatto energetico, integrate nei cruscotti *SupTech*; lo sviluppo di un *corpus* di diritto digitale sostanziale, capace di riconoscere e sanzionare derive tecnocratiche e di proteggere l'autonomia dei soggetti; la promozione di un programma transnazionale di formazione ibrida, per far dialogare filosofi del diritto, giuristi, ingegneri e *data scientist*; l'implementazione di meccanismi di valutazione *ex ante* ed *ex post*, ispirati al modello del *Regulatory Impact Assessment*, adattati al contesto algoritmico; e, infine, la creazione di un Registro pubblico dei modelli *RegTech* e *SupTech* certificati, per favorire la condivisione delle *best practice* e l'evoluzione continua del quadro tecnologico e normativo.

Solo attraverso un impegno concertato e multilivello – che traduca la visione valoriale della Carta in linee di *policy* e in architetture tecniche pienamente inte-

[63] Il termine si riferisce a un concetto emergente nel dibattito giuridico e politologico che esplora come i valori e i principi fondamentali del costituzionalismo tradizionale (come lo stato di diritto, la separazione dei poteri, la tutela dei diritti umani, la democrazia) debbano essere riaffermati e adattati all'era digitale e alla *governance* delle tecnologie. Nel presente contesto, si vuole descrivere l'idea di un'evoluzione necessaria in cui principi quali trasparenza, responsabilità e consultazione pubblica non rimangono mere dichiarazioni d'intenti, ma vengano concretamente integrati nelle architetture tecniche e nei processi dei sistemi digitali (come le piattaforme *RegTech/SupTech*), al fine di prevenire derive tecnocratiche e rischi per i diritti fondamentali. Questa prospettiva va oltre la semplice regolamentazione delle tecnologie per proporre un vero e proprio quadro costituzionale per lo spazio digitale, tenendo conto dei poteri esercitati non solo dagli Stati ma anche da attori privati (come le grandi piattaforme digitali). È un campo di ricerca in rapida crescita nel quale si incontrano diverse discipline. Si veda, ad esempio, E. Celeste, *Digital Constitutionalism. The Role of Internet Bills of Rights*, London, 2022; G. De Gregorio, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022. Il concetto si lega anche alle riflessioni sull'impatto della tecnologia sul diritto e sulla forma dello Stato, sviluppate nella dottrina italiana e già più volte citate nel presente lavoro.

grate – l'Europa potrebbe condurre la trasformazione digitale verso un modello di *governance* realmente sostenibile, inclusivo e giusto, evitando che i rischi di *bias*, asimmetrie informative e sovraccarico energetico compromettano la promessa di diritti digitali effettivi per tutti.

N. 3 - 2025 - pp. 40-52

# L'architettura normativa dei diritti digitali nella Dichiarazione europea per il decennio digitale: principi fondamentali e nuove regolamentazioni nel quadro di un costituzionalismo digitale europeo

**Andrea Lisi - Sarah Ungaro**

**Abstract:** Il presente contributo si propone di esaminare, attraverso un approccio analitico rigoroso, i contenuti e le implicazioni giuridiche dei capitoli III e V della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, adottata il 15 dicembre 2022 dalle istituzioni dell'Unione Europea. L'indagine si concentra sulla complessa articolazione tra libertà di scelta nell'ecosistema digitale e sicurezza, protezione e conferimento di maggiore autonomia responsabile, evidenziando le tensioni dialettiche e le sfide ermeneutiche che connotano l'implementazione di tali principi nella prassi giuridica contemporanea.

This paper aims to examine, through a rigorous analytical approach, the content and legal implications of Chapters III and V of the European Declaration on Digital Rights and Principles for the Digital Decade, adopted on 15 December 2022 by the European Union institutions. The investigation focuses on the complex interplay between freedom of choice in the digital ecosystem and security, protection, and the granting of greater responsible autonomy, highlighting the dialectical tensions and hermeneutical challenges that characterize the implementation of these principles in contemporary legal practice.

**Parole chiave:** principi fondamentali, intelligenza artificiale, protezione dei dati personali, condivisione dei dati, costituzionalismo digitale.

# 1. Riflessioni preliminari sulla strategia della trasformazione digitale europea

L'avvento dell'era digitale ha determinato una trasformazione epocale delle relazioni sociali, economiche e giuridiche, imponendo ai legislatori e agli interpreti del diritto lo sforzo ermeneutico di governare la complessità della realtà digitale, rileggendo le categorie concettuali tradizionali con un nuovo rigore metodologico. In questo contesto, la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale si configura come un documento di straordinaria rilevanza, in quanto delinea l'architettura normativa attraverso la quale l'Unione Europea intende governare la transizione digitale secondo un approccio antropocentrico, etico e valoriale.

Il terzo Considerando del Preambolo della Dichiarazione enfatizza come "la trasformazione digitale non dovrebbe comportare la regressione dei diritti" e stabilisce il principio fondamentale secondo cui "ciò che è illegale offline è illegale online", configurando così un continuum normativo tra dimensione fisica e digitale che preservi l'integrità dell'ordinamento giuridico europeo.

I capitoli III e V della Dichiarazione, oggetto della presente analisi, rappresentano due cardini essenziali di questa costruzione teorica: il primo articola il principio della libertà di scelta nell'ambiente digitale, mentre il secondo delinea i parametri della sicurezza, protezione e maggiore autonomia e responsabilità nell'ambiente digitale. La loro analisi congiunta rivela la complessità delle sfide che l'ordinamento europeo deve affrontare per conciliare l'esigenza di non pregiudicare la trasformazione digitale e di favorire lo sviluppo del mercato unico digitale con quella di garantire un ambiente digitale sicuro e protetto, salvaguardando la dimensione umana nell'ecosistema digitale.

Proprio in tema di mercato unico digitale, risulta evidente come siano proprio i dati (personali e non personali) a rappresentare la risorsa più importante e più appetibile in questa fase storica dell'economia, non solo europea. In tal senso, appare utile effettuare un parallelismo tra l'odierno momento storico, in cui l'Unione europea cerca di costruire una strategia europea di condivisione dei dati nel contesto digitale[1], e uno dei primi accordi che hanno costituito le fondamenta su cui

[1] Si veda, in tal senso, il documento della Commissione europea del 2020 per la Strategia europea per i dati. In particolare, la Commissione specifica che: "*L'obiettivo è creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore* (omissis). *Dovrebbe trattarsi di uno spazio nel quale il diritto dell'UE possa essere applicato con efficacia e nel quale tutti i prodotti e i servizi*

si basa oggi l'odierna Unione, ossia il Trattato di Parigi, o Accordo CECA, firmato il 18 aprile 1951, che istituì la Comunità Europea del Carbone e dell'Acciaio. Se, in effetti, nel 1951 le materie prime fondamentali per lo sviluppo del mercato unico europeo erano il carbone e l'acciaio, oggi sono i dati a costituire la "materia prima" e la risorsa più importante per lo sviluppo economico dell'Unione, attesa l'importanza strategica del mercato dei servizi digitali (basti pensare alle piattaforme e alle risorse digitali attraverso cui sono trattati dati di enti e soggetti pubblici, aziende, comunicazioni istituzionali, servizi essenziali, tra cui quelli sanitari, etc.): per tali motivi, nell'attuale contesto digitale, sono i dati ad essere oggetto di una strategia europea di condivisione[2].

## 2. I temi del Capitolo III della Dichiarazione: la dialettica assiologica tra libertà di scelta ed efficientismo tecnocratico negli ecosistemi digitali

Il Capitolo III della Dichiarazione si apre con una proclamazione di principio di straordinaria pregnanza concettuale: "L'intelligenza artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano". Questa formulazione rivela l'intenzione del Legislatore europeo di subordinare inequivocabilmente lo sviluppo tecnologico alle finalità umane, rovesciando la prospettiva ostentatamente efficientistica e tecnocratica che spesso caratterizza l'approccio alla trasformazione digitale e, nell'ultimo periodo, all'intelligenza artificiale.

Tale prospettiva, peraltro, è stata poi oggetto di ulteriore conferma nell'art. 1 dell'AI Act, in cui si rivela la ratio legis con straordinario nitore, specificando che lo scopo del Regolamento è quello di "migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile"[3].

*basati sui dati siano conformi alle pertinenti normative del mercato unico dell'UE. Quest'ultima dovrebbe a tal fine combinare una legislazione e una governance idonee allo scopo per garantire la disponibilità dei dati, investendo in norme, strumenti e infrastrutture, come pure in competenze per la gestione dei dati*".

[2] Per approfondimenti sul tema si segnala l'intervento del Prof. Donato Limone, "La complessità della sicurezza digitale" nell'ambito del seminario "NIS2, sicurezza e autenticità dei dati", 18 luglio 2025, disponibile sulla piattaforma Digeat all'indirizzo https://digeat.info/, in cui l'Autore pone in luce acutamente come, nella fase storica attuale, non possa esserci una vera Unione europea degli Stati senza un'Unione europea dei dati.

[3] Per completezza, di seguito si riporta il testo del par. 1, art. 1 del Regolamento (UE) 2024/1689 del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza

Le motivazioni poste a fondamento di tale impostazione risiedono nella consapevolezza che l'intelligenza artificiale, per la sua capacità di influenzare profondamente i processi decisionali individuali e collettivi, può non essere considerata uno strumento neutrale nel suo materiale sviluppo e nei suoi effetti concreti, sia in ragione di bias derivanti da elementi caratterizzanti gli input, ossia la fase di alimentazione e prompting, sia in ragione degli effetti negativi che gli output frutto dell'utilizzo di tali sistemi possono avere sui diritti fondamentali delle persone, in particolare per i sistemi di IA ad alto rischio[4] o per i modelli di IA con finalità generali aventi rischio sistemico[5].

Tuttavia, non si possono sottacere i limiti della formulazione di questa norma, in cui probabilmente il Legislatore europeo ha voluto imprimere una connotazione addirittura teleologica ai sistemi di intelligenza artificiale, non ritenendo invece di dover stabilire esplicitamente come condizione necessaria e inderogabile che gli stessi siano sviluppati in modo da garantire il rispetto dei diritti fondamentali (poiché si prevede pure che l'entità dell'eventuale lesione degli stessi debba essere semplicemente oggetto di una valutazione del rischio).

Pertanto, il riferimento al "benessere umano" come obiettivo ultimo, espressamente inserito nell'incipit del Capitolo III della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, non dovrebbe essere interpretato come una dichiarazione programmatica, ma quale parametro assiologico attraverso il quale valutare la legittimità e l'opportunità dei risultati offerti da tali sistemi che sono alla base di una profonda trasformazione dei fenomeni economici, sociali, giuridici in tutti i contesti.

In tale prospettiva, un aspetto particolarmente significativo della disciplina contenuta nel Capitolo III concerne l'articolazione del principio di trasparenza algoritmica. La Dichiarazione stabilisce l'impegno a "garantire un livello adeguato di trasparenza in merito all'uso degli algoritmi e dell'intelligenza artificiale e fare in modo che le persone siano autonome e responsabili quando li utilizzano e informate quando interagiscono con essi".

artificiale): "*Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione*".

[4] Si veda il Capo III dell'AI Act.

[5] Cfr. art. 51 dell'AI Act. Ai sensi dell'art.3, n. 65) dello stesso Regolamento, per «rischio sistemico» si intende un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore.

Tale previsione implica un superamento del paradigma della "black box algoritmica", introducendo un diritto alla comprensibilità dei processi decisionali automatizzati che incidono sulla sfera giuridica degli individui. La trasparenza algoritmica non si configura meramente come un diritto all'informazione, ma come condizione necessaria per l'esercizio dell'autonomia decisionale nell'ambiente digitale.

La formulazione adottata dal Legislatore europeo rivela una concezione sofisticata dell'autonomia individuale, che non si limita alla mera libertà di scelta formale, ma richiede la presenza di condizioni sostanziali che rendano tale scelta effettivamente libera e consapevole. L'informazione diviene così presupposto indefettibile dell'autonomia, secondo una logica che rievoca i principi del diritto dell'interessato ad essere informato sul trattamento dei dati personali attualmente codificato nel GDPR[6], a partire dall'art. 5, par. 1, lett. a), che sancisce il principio di trasparenza nel trattamento de dati, ovviamente negli artt. 12, 13 e 14 dello stesso Regolamento, dedicati alle informazioni da rendere disponibili all'interessato, ma anche in altre disposizioni, come nell'art. 26 GDPR, che stabilisce che i contitolari siano tenuti a portare a conoscenza degli interessati il contenuto essenziale dell'accordo di contitolarità.

Dal principio di trasparenza discende un corollario specifico, ossia il principio di spiegabilità delle decisioni dei sistemi di IA, enucleato nel Considerando 27 dell'AI Act: sulla scorta di tale principio, la trasparenza nei sistemi di IA è declinata in logiche di sviluppo e utilizzo idonee a consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i deployer delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti.

Sul tema, appare utile segnalare una recentissima pronuncia del Consiglio di Stato, sezione VI, 6 giugno 2025, n. 4929 – Pres. De Felice, Est. Ponte, in cui si è ribadito che il diritto di accesso non può essere negato a causa di difficoltà conoscitive derivanti dall'utilizzo, nell'esercizio dell'attività amministrativa, di algoritmi interamente gestiti in forma automatizzata[7].

---

[6] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[7] In particolare, i Giudici di Palazzo Spada hanno evidenziato che l'utilizzo di sistemi di intelligenza artificiale, dagli algoritmi al c.d. machine learning, va inteso quale modulo procedimentale per lo svolgimento dell'attività autoritativa in modalità più efficienti ed è regolato dai principi di conoscibilità e comprensibilità, non esclusività della decisione algoritmica, non discriminazione algoritmica; pertanto, l'amministrazione dotata di competenza primaria nella materia della gestione e del pagamento dei contributi oggetto di un'istanza di accesso non può trincerarsi dietro la non conoscibilità dei meccanismi informatici di gestione: alla luce dei suddetti principi, a chi chiede l'accesso non sono opponibili le difficoltà conoscitive derivanti dall'utilizzo, nell'esercizio

Un elemento di particolare rilievo nella disciplina dell'intelligenza artificiale contenuta nel Capitolo III della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale è rappresentato dalla previsione della sorveglianza umana. Il documento stabilisce che "i sistemi algoritmici siano basati su insiemi di dati adeguati al fine di evitare discriminazioni e consentano la supervisione umana di tutti i risultati che interessano la sicurezza e i diritti fondamentali delle persone".

Questa disposizione introduce un principio di inderogabilità della componente umana nei processi decisionali che incidono su interessi giuridicamente rilevanti. La sorveglianza umana non si configura come mero controllo ex post, ma come elemento strutturale del processo decisionale automatizzato - che si ritrova sia nell'AI Act, in particolare nell'art. 14 con riferimento ai sistemi ad alto rischio[8], sia nel GDPR, all'art. 22[9] – ed è volto a garantire che i rischi derivanti dai processi decisionali automatizzati possano essere mitigati dall'elemento della sorveglianza umana[10].

dell'attività amministrativa, di algoritmi interamente gestiti in forma automatizzata. Si consiglia, in proposito, la lettura del contributo a firma di Carola Caputo, dal titolo "La conoscibilità dei sistemi di IA come corollario della trasparenza amministrativa", pubblicato nell'agosto 2025, sulla Rivista "Agendadigitale.eu", testata scientifica ISSN 2421-4167.

[8] Art. 14 AI Act:

1. *I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.*
2. *La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti* (omissis).

[9] Articolo 22 GDPR, *Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione*

1. *L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.*
2. *Il paragrafo 1 non si applica nel caso in cui la decisione:*
   *a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;*
   *b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;*
   *c) si basi sul consenso esplicito dell'interessato.*
3. *Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.*
4. *Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.*

[10] Tra le misure di sorveglianza umana, l'art. 14, par. 4, dell'AI Act menziona le seguenti:

a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e

Inoltre, il riferimento specifico alla necessità di evitare discriminazioni attraverso l'utilizzo di "insiemi di dati adeguati"[11] rivela la consapevolezza del Legislatore europeo circa i rischi di perpetuazione e amplificazione di bias discriminatori attraverso l'utilizzo di algoritmi di machine learning. Tale previsione si inscrive in una più ampia strategia di tutela dell'uguaglianza sostanziale nell'ambiente digitale, che richiede un'attenzione particolare sia alla qualità dei dati sia ai meccanismi attraverso i quali i pregiudizi sociali possono essere incorporati nei sistemi tecnologici.

Sotto diverso profilo, il Capitolo III della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale si sofferma con significativo interesse sulla configurazione di un ambiente digitale equo, caratterizzato dalla promozione della concorrenza e dell'innovazione, nella chiara prospettiva di valorizzare gli obiettivi economici che sono stati successivamente delineati nella richiamata Strategia europea per i dati, in primis la creazione di un mercato unico europeo di dati e di servizi digitali.

In particolare, la Dichiarazione, al Capitolo III, par. 11, lett. a), stabilisce l'im-

affrontare anomalie, disfunzioni e prestazioni inattese;

b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio («distorsione dell'automazione»), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche;
c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;
d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio;
e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di «arresto» o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.

Più in generale, il Considerando 73 dell'AI Act precisa che le misure di sorveglianza umana "dovrebbero in particolare garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo. È inoltre essenziale, se del caso, garantire che i sistemi di IA ad alto rischio includano meccanismi per guidare e informare la persona fisica alla quale è stata affidata la sorveglianza umana affinché prenda decisioni informate in merito alla possibilità, ai tempi e alle modalità di intervento, onde evitare conseguenze negative o rischi, oppure affinché arresti il sistema, qualora non funzionasse come previsto. Tenuto conto delle conseguenze significative per le persone in caso di una corrispondenza non corretta da parte di determinati sistemi di identificazione biometrica, è opportuno prevedere un requisito rafforzato di sorveglianza umana per tali sistemi, in modo che il deployer non possa adottare alcuna azione o decisione sulla base dell'identificazione risultante dal sistema, a meno che ciò non sia stato verificato e confermato separatamente da almeno due persone fisiche. Tali persone potrebbero provenire da una o più entità e comprendere la persona che gestisce o utilizza il sistema. Tale requisito non dovrebbe comportare oneri o ritardi inutili e potrebbe essere sufficiente che le verifiche separate da parte delle diverse persone siano automaticamente registrate nei log generati dal sistema".

[11] Si veda il Capitolo III, par. 9, lett. c) della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale.

pegno a "garantire un ambiente digitale sicuro e protetto, basato sulla concorrenza leale, in cui siano tutelati i diritti fondamentali, siano garantiti i diritti degli utenti e la protezione dei consumatori nel mercato unico digitale e siano ben definite le responsabilità delle piattaforme, in particolare dei grandi operatori e dei gatekeeper".

Questa previsione rivela una concezione dell'equità digitale che trascende la mera tutela dei diritti individuali per abbracciare una dimensione sistemica, volta a preservare le condizioni strutturali di un intero ecosistema di servizi per il funzionamento di un mercato concorrenziale di servizi e di dati (che ne costituiscono la risorsa primaria) digitali. Nello specifico, si rileva che il riferimento ai "grandi operatori" e "ai gatekeeper"[12] evidenzia la consapevolezza del Legislatore europeo circa i rischi di concentrazione del potere economico nell'ecosistema digitale in mano a grandi operatori di mercato che agiscono, sostanzialmente, in regime di oligopolio, e la necessità di adottare misure specifiche per contrastare l'emergere di posizioni dominanti.

## 3. Capitolo V della Dichiarazione: sicurezza, protezione e responsabilizzazione nell'ecosistema digitale

Il Capitolo V della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale delinea un modello di sicurezza che si caratterizza per l'adozione di un approccio preventivo e sistemico. Il documento, al par. 16, stabilisce che "ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione, traducendosi in un

[12] I gatekeeper sono piattaforme digitali di grandi dimensioni che offrono una serie predefinita di servizi digitali, definite come "servizi di piattaforma essenziali", quali motori di ricerca online, app store e servizi di messaggistica. Queste piattaforme:

- detengono una posizione economica forte, hanno un impatto significativo sul mercato interno e operano in più paesi dell'UE;
- occupano una forte posizione di intermediazione, nel senso che collegano un'ampia base di utenti a un gran numero di imprese;
- hanno una posizione consolidata e duratura sul mercato, vale a dire stabile nel tempo.

Tali soggetti sono destinatari degli obblighi previsti dal Digital Markets Act, di cui Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).
Il 6 settembre 2023 la Commissione europea ha designato per la prima volta sei gatekeeper: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, che offrono molti dei servizi di piattaforma essenziali (per approfondimenti, si rimanda al sito web della Commissione europea https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_it).

elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate".

L'espresso riferimento alla tutela della "vita privata fin dalla progettazione" richiama un principio già presente nell'ordinamento europeo, che è quello della privacy by design, che nel GDPR è già sancito all'art. 25 e che si affianca al principio della privacy by default. Tale approccio riflette una concezione della protezione dei dati personali che non si limita alla regolamentazione del trattamento, ma si estende alla progettazione stessa dei servizi e delle architetture tecnologiche che implicano il trattamento dei dati personali, adottando le misure di sicurezza volte ad attuare in modo efficace i principi di protezione dei dati, e in modo che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Inoltre, la Dichiarazione anticipa la previsione dei quattro parametri di sicurezza (riservatezza, integrità, disponibilità e autenticità), rivelando l'adozione di una prospettiva sistemica della cybersecurity, che abbraccia tanto la dimensione tecnica quanto quella giuridica della protezione delle informazioni e che successivamente sarà confermata nell'impostazione delle norme della Direttiva NIS 2[13]. Tale Direttiva, insieme al D.Lgs. 138/2024[14] che ne recepisce le disposizioni nell'ordinamento italiano, delinea un quadro normativo rafforzato per la protezione dei dati e la resilienza delle infrastrutture digitali, ricomprendendo espressamente per la prima volta l'autenticità dei dati[15] quale ulteriore elemento cruciale nel contesto della cybersecurity, esaminando i rischi correlati alla sua compromissione e alla sua interdipendenza con i più noti principi fondamentali della triade RID (o CIA) della sicurezza, relativa ai fattori della Riservatezza (Confidentiality), dell'Integrità (Integrity) e della Disponibilità (Availability).

Un ulteriore aspetto di particolare rilevanza nella disciplina contenuta nel Capitolo V della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale concerne l'articolazione del principio di controllo individuale sui dati personali. Al par. 17, la Dichiarazione stabilisce che "ogni persona ha diritto al rispetto della vita privata e alla protezione dei propri dati personali. Quest'ultimo diritto

[13] Direttiva (UE) 2022/2555 del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (Direttiva NIS 2).

[14] Decreto Legislativo 4 settembre 2024, n. 138, Recepimento della Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148.

[15] L'autenticità è definibile come quell'elemento che esprime la garanzia che i dati siano attribuibili (e le relative azioni/conseguenze siano giuridicamente imputabili) ai soggetti ai quali gli stessi dati risultino riconducibili e ascrivibili, escludendo inoltre che possano essere stati modificati da soggetti non autorizzati.

prevede anche che i singoli individui abbiano il controllo di come sono utilizzati i propri dati e con chi sono condivisi".

Questa formulazione introduce una concezione dell'autodeterminazione informativa che trascende la mera tutela della riservatezza per abbracciare una dimensione di controllo attivo sui propri dati. Il diritto al controllo non si limita alla facoltà di opporsi al trattamento, ma si estende alla possibilità di determinare le modalità e le finalità dell'utilizzo delle informazioni personali.

Sul tema, risulta ovvio fare riferimento al diritto alla portabilità dei dati personali, sancito all'art. 20 GDPR, che nella Dichiarazione in commento viene contemplato, con un'accezione più generale, attraverso l'impegno a "garantire l'effettiva possibilità per i singoli individui di trasferire facilmente i propri dati personali e non personali tra diversi servizi digitali" (par. 19, lett. b, del Capitolo V della Dichiarazione). In tale prospettiva, dunque, la portabilità dei dati non costituisce meramente un diritto individuale, ma un meccanismo per promuovere la concorrenza nell'ecosistema digitale, riducendo i costi di trasferimento e contrastando l'emergere del noto effetto "lock-in".

Peraltro, anche nel Regolamento europeo eIDAS 2[16], dedicato all'identità digitale e ai servizi fiduciari, in cui è stato recentemente introdotta la disciplina del c.d. wallet europeo, ossia del "portafoglio digitale" attraverso i cui servizi sarà possibile attestare l'identità di una persona fisica o giuridica e i relativi attributi e qualifiche, sono state previste disposizioni dedicate a ciò che viene definito come un "pannello di gestione" dei dati personali. In particolare, tale pannello di gestione dovrebbe consentire agli utenti anche di "segnalare facilmente la parte facente affidamento sulla certificazione all'autorità nazionale di protezione dei dati competente qualora sia ricevuta una richiesta di dati personali presumibilmente illecita o sospetta", integrando un ulteriore esempio di controllo sull'utilizzo e condivisione dei dati già previsto nella Dichiarazione europea sui diritti e i principi digitali per il decennio digitale.

Il Capitolo V della Dichiarazione, inoltre, dedica particolare attenzione alla tutela della riservatezza delle comunicazioni, stabilendo che "ogni persona ha diritto alla riservatezza delle proprie comunicazioni e delle informazioni sui propri dispositivi elettronici e a non essere sottoposta a sorveglianza online illecita, tracciamento pervasivo illecito o misure di intercettazione".

Tale previsione introduce nell'ordinamento europeo un diritto alla confiden-

[16] Regolamento UE 2014/910 del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, così come novellato dal Regolamento UE 2024/1183 dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

zialità digitale che si configura come estensione del tradizionale diritto alla riservatezza delle comunicazioni. Il riferimento specifico al "tracciamento pervasivo illecito" evidenzia la consapevolezza del Legislatore europeo circa i rischi derivanti dall'utilizzo di tecnologie di profilazione invasive, che possono compromettere l'autonomia individuale attraverso la creazione di un ambiente di sorveglianza diffusa.

In relazione a tali profili, tuttavia, occorre rilevare che risulta ancora fermo l'iter di approvazione del c.d. Regolamento e-privacy[17]: in effetti, fin dal 2017 la Commissione europea ha adottato la proposta di regolamento relativo alla vita privata e alle comunicazioni elettroniche, ma lo stesso risulta arenato, probabilmente per via dei rilevanti impatti che le disposizioni ivi previste avrebbero sul mercato dei servizi digitali, qualora entrassero in vigore[18].

# 4. Conclusioni: principi fondamentali e nuove regolamentazioni nel quadro di un costituzionalismo digitale europeo

L'analisi congiunta dei Capitoli III e V della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale rivela l'esistenza di tensioni dialettiche significative tra l'esigenza di garantire i diritti e le libertà delle persone nell'ambiente digitale e quella di favorire il più possibile la condivisione dei dati per lo sviluppo di un mercato unico di servizi digitali nell'Unione. Tale tensione, tuttavia, non costituisce necessariamente una contraddizione, ma riflette la complessità intrinseca della regolazione dell'ecosistema digitale.

In effetti, tali tensioni dialettiche che emergono dalla lettura delle disposizioni della Dichiarazione delineano i contorni di un quadro di principi, definibile come una sorta di costituzionalismo digitale[19] europeo: in questa prospettiva, solo uno sforzo ermeneutico attento da parte degli interpreti del diritto può permettere di preservare e promuovere i valori fondamentali dell'ordinamento europeo nell'am-

---

[17] Proposta di Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (Regolamento sulla vita privata e le comunicazioni elettroniche), il cui testo è reperibile al link https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications.

[18] Per approfondimenti si rimanda ai contenuti della Commissione europea disponibili al link https://digital-strategy.ec.europa.eu/it/policies/eprivacy-regulation.

[19] L'espressione "digital constitutionalism" risulta attribuibile a una ricerca pubblicata nel 2015 dal Berkman Center for Internet and Society dell'Università di Harvard, disponibile al link https://dash.harvard.edu/entities/publication/73120378-fb52-6bd4-e053-0100007fdf3b.

biente digitale, evitando sia il rischio di un interventismo regolatorio eccessivamente restrittivo sia quello di una deriva di efficientismo tecnocratico.

In questa prospettiva, la Dichiarazione si configura come tappa fondamentale di un processo evolutivo della normazione che trova approdo nelle regolamentazioni specifiche, a partire dal GDPR, e nei successivi Regolamenti e Direttive emanati nell'ambito della Strategia europea dei dati e che dovrà necessariamente confrontarsi con le sfide emergenti dell'innovazione tecnologica, mantenendo saldo l'ancoraggio ai principi fondamentali dell'Unione europea.

Tuttavia, in questo complesso scenario di costituzionalizzazione di principi e diritti digitali sviluppati nella visione programmatica della Dichiarazione, occorre rilevare che non sono effettivamente ricomprese le fondamentali garanzie offerte dalle Autorità indipendenti, che dovrebbero essere preposte alla vigilanza sull'applicazione effettiva dei principi e dei diritti digitali sanciti nella Dichiarazione.

Tale circostanza non appare essere una semplice dimenticanza del Legislatore europeo: in tal senso, non si può non osservare che l'inclusione di un esplicito richiamo alla garanzia di un'Autorità indipendente nella Dichiarazione avrebbe introdotto la codificazione di un diritto fondamentale in modo trasversale e generale, che avrebbe dovuto essere conseguentemente declinato e recepito in tutte le successive regolamentazioni specifiche aventi un impatto nel contesto digitale. In effetti, al momento, tale garanzia è prevista solo con riferimento al diritto alla protezione dei dati personali, il cui rispetto, secondo l'art. 8 della Carta dei diritti fondamentali dell'Unione europea, "è soggetto al controllo di un'autorità indipendente"[20].

Pertanto, è possibile dedurre che sia stato proprio il processo di "costituzionalizzazione" del diritto alla protezione dei dati personali ad aver determinato la scelta del Legislatore europeo di affidarne il controllo ad un'Autorità indipendente.

Attualmente, si sottolinea la tendenza a una proliferazione di Authority (anche in riferimento all'intelligenza artificiale, disciplinata nell'AI Act), circostanza che di fatto genera complessità di azione, ma che al contempo costituisce causa ed effetto di una certa "settorializzazione" dei diritti nei diversi ambiti della realtà digitale.

---

[20] Art. 8 della Carta dei diritti fondamentali dell'Unione europea
Protezione dei dati di carattere personale
1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Nel prossimo futuro, sarà possibile verificare se il Legislatore europeo intenda disciplinare tali aspetti ricomprendendo in un alveo più propriamente giurisdizionale e garantista anche la tutela specifica degli altri diritti digitali sanciti nella Dichiarazione, nel quadro di un costituzionalismo digitale europeo.

N. 3 - 2025 - pp. 53-60

# La reale attuazione di principi e diritti digitali in Italia

**Giovanni Manca**

**Abstract**: La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01) è fondamentale per orientare le scelte di natura sociale per un mondo che è già ampiamente digitale e con l'intelligenza artificiale tende a esserlo ancora di più occupando gli spazi della persona. L'espressione diritti digitali è anche seducente, se il mondo è digitale anche la persona deve disporre e reclamare i propri diritti.
In Italia a partire dai primi anni '90 la legislatura ha sempre di più sviluppato il tema di amministrazione digitale della società. Una indiscutibile pietra miliare è il Codice dell'amministrazione digitale (CAD – Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni) che peraltro, nel tempo ha perso l'obiettivo di essere principio, scivolando sempre di più verso lo stato di contenitore di norme, anche attuative, da inserire "al volo" per legiferare sui temi del momento. Alla data di marzo 2025 il sito di Normattiva ci informa che sono 509 le modifiche rispetto al testo originale.
Nonostante le premesse possono sembrare negative l'amministrazione digitale per cittadini, imprese e professionisti avanza costantemente e le novità nella vita quotidiana sono, forse, anche troppe. Un interessante esercizio che svolgiamo in questa sede è l'analisi di quanto i diritti e i principi digitali siano attuati in Italia e quanto questa attuazione sia reale oppure teorica, inefficace, inefficiente e conseguentemente non economicamente sostenibile.

The European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01) is essential to guide social choices for a world that is already largely digital and with artificial intelligence tends to be even more so by occupying the spaces of the person. The expression digital rights is also seductive, if the world is digital, the person must also have and claim their rights.
In Italy, starting from the early 90s, the legislature has increasingly developed the theme of digital administration of society. An indisputable milestone is the Digital Administration Code (CAD - Legislative Decree 7 March 2005, n. 82 and subsequent amendments) which, however, over time has lost the objective of being a principle,

slipping more and more towards the state of container of rules, including implementing ones, to be inserted “on the fly” to legislate on the issues of the moment. As of March 2025, the Normattiva website informs us that there are 509 changes compared to the original text.
Although the premises may seem negative, digital administration for citizens, businesses and professionals is constantly advancing and the innovations in daily life are, perhaps, even too many. An interesting exercise that we carry out here is the analysis of how digital rights and principles are implemented in Italy and how much this implementation is real or theoretical, ineffective, inefficient and consequently not economically sustainable.

**Parole chiave:** principi digitali, diritti digitali, stato dell’arte, attuazione, risultati.



# 1. I principi e diritti digitali

La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale è senz’altro una iniziativa importante dell’Unione Europa per disporre di una base di partenza utile a guidare la trasformazione digitale in linea con i valori europei.

Le potenziali utilità sono varie e in particolare:

- ✓ stabilisce un quadro di riferimento istituzionale sui diritti digitali, colmando un vuoto normativo in un settore in costante e rapida evoluzione;
- ✓ protegge i cittadini promuovendo principi come la protezione dei dati personali, la cybersecurity e l’inclusione digitale;
- ✓ fornisce un riferimento di base comune per le politiche digitali nei vari stati membri.

La sua applicazione pratica nella variegata società europea è tangibile per la sua influenza sulle politiche digitali europee che hanno trovato attuazione con numerose norme che legiferano su questi principi come il *Digital Services Act* e il *Digital Markets Act*.

Tuttavia, l’implementazione effettiva varia tra i diversi Stati membri.
In alcuni settori ed aree geografiche l’applicazione è più visibile e diffusa con:

- regolamentazione delle piattaforme digitali;

- protezione dei dati personali;
- iniziative per l'inclusione digitale;

Le criticità non mancano considerato il settore in rapida evoluzione e mutazione e nell'area dell'Unione caratterizzata da numerosi Stati e da differenti culture sulla trasformazione digitale.

Queste premesse causano:

- disomogeneità nella digitalizzazione tra le diverse regioni europee;
- difficoltà nel bilanciare innovazione e regolamentazione;
- sfide nell'applicazione pratica per trovare equilibrio con le grandi aziende tecnologiche.

In sintesi, la dichiarazione è certamente un passo importante per definire un modello europeo di digitalizzazione centrato sulla persona, ma il suo impatto reale non può che dipendere dalla capacità di tradurre questi principi in azioni concrete e vincolanti.

Questa situazione è presente anche in Italia dove il tema non è se esiste digitalizzazione ma come questa è attuata e il bilancio sociale della sua attuazione.

La saggezza popolare ci ricorda che il tempo è galantuomo e noi ricordiamo, citando tre pilastri della trasformazione digitale che il documento informatico esiste dal 1993, la firma digitale dal 1997 e l'identità digitale dal 2016. Questi pilastri sono la base per solidi edifici di attuazione del digitale o solo fuochi fatui frutto di mode del momento divenuti meri adempimenti burocratici?

Proviamo ad analizzare la stato dell'arte per comprendere il livello dell'attuazione italiana dei diritti e dei principi.

## 2. L'attuazione italiana dei singoli diritti e principi

La nostra analisi è puntuale rispetto al testo della dichiarazione che utilizziamo come base per i commenti sopra descritti. Il cortese lettore è rinviato al testo ufficiale della dichiarazione che non viene esplicitamente citato (salvo alcuni indispensabili elementi) per non appesantire l'esposizione dei commenti.

Iniziamo con il CAPITOLO I dedicato alla centralità della persona rispetto alla trasformazione digitale. Il principio è ineccepibile e base essenziale per l'applicazio-

ne dei valori dell'Unione e i diritti delle persone riconosciuti dal diritto dell'Unione.

Nel CAD, mescolati nel contenitore dell'amministrazione digitale, ci sono il diritto all'uso delle tecnologie e l'identità e il domicilio digitale associati entrambi alla Carta della cittadinanza digitale. Introdurre nel preambolo di questa norma il riferimento alla dichiarazione dei diritti e dei principi non sarebbe un errore.

Nel CAPITOLO II dedicato alla solidarietà e all'inclusione si enunciano ulteriori concetti basilari nei valori dell'Unione rispetto ai diritti fondamentali con attenzione alla solidarietà e l'inclusione. La trasformazione digitale deve realizzare la parità di genere e includere in particolare gli anziani. Su quest'ultimo punto sta crescendo l'attenzione con la classica assistenza territoriale che si sta focalizzando sui "Punti Digitale Facile" finanziati con fondi PNRR. L'obiettivo 2026 è per circa due milioni di cittadini da assistere con oltre 3000 punti sul territorio.

La comunicazione è supportata anche con uno spot di ampia diffusione ma per sapere dove sono i punti bisogna avere pratica di informatica sul sito e nei grandi centri non è facile individuare quello vicino all'abitazione dell'interessato.

Il tema connettività è il più importante nell'ambito delle infrastrutture tecnologiche. In ogni luogo, ogni persona dovrebbe avere accesso alla connettività digitale ad alta velocità (come si dice abitualmente connessione a banca larga) con prezzi accessibili.

Senza adeguata connettività non possono essere erogati servizi cloud adeguati, le zone svantaggiate non sono attrattive per lo *smart working* e i servizi "di diritto" non possono essere di qualità.

La situazione italiana è ottima in alcune zone e pessima in molte altre. Si continua ad operare per migliorare la situazione e AGCOM continua a segnare miglioramenti ma anche lentezza nelle aree cosiddette nere e grigie. Situazione peggiore per la banda ultra larga ma anch'essa in miglioramento, forse troppo lentamente.

Deve essere sostenuta con forza una rete neutra senza blocchi o degrado di servizi e contenuti.

In ambito educazione digitale e competenze, l'istruzione, la formazione e l'apprendimento permanente nell'ambito digitale devono essere diritti fondamentali.

In Italia si comincia a parlare di istruzione digitale sin dai primi anni di scuola e si sta lavorando anche per l'inclusione e per colmare il divario digitale di genere. Probabilmente l'inerzia nell'utilizzo dei servizi digitali da parte della popolazione, a qualunque titolo, ha accelerato la difficoltà del mondo caratterizzato dal divario

digitale anche per una qualità ed efficienza dei servizi in rete ancora da migliorare.

Il diritto a condizioni di lavoro eque, giuste e sicure anche nell'ambiente digitale è indispensabile. In fase di sviluppo della consapevolezza e oggetto di giusta attenzione è il diritto alla disconnessione, all'equilibrio tra vita professionale e privata, e alla protezione dalla sorveglianza illecita sul posto di lavoro. La vicenda della pandemia ha evidenziato notevolmente questi aspetti ma bisogna essere operativi e pragmatici soprattutto con l'avanzare dell'intelligenza artificiale.

La diffusione dei servizi pubblici digitali deve essere diffusa e ogni persona dovrebbe avere accesso online ai servizi pubblici principali nell'UE, attraverso un'identità digitale accessibile, volontaria e sicura, con particolare attenzione ai servizi sanitari e assistenziali digitali. Il sistema SPID e la sua convergenza verso il Portafoglio Europeo di Identità Digitale sono la risposta a questi temi. Con la piena operatività del portafoglio sarà indispensabile avere uno scenario di servizi coordinato con questo sfruttando il vantaggio di una identità digitale unica, interoperabile e allo stato dell'arte nella cybersicurezza e nella protezione dei dati personali.

Il CAPITOLO III tratta della libertà di scelta degli individui nell'ambito delle tecnologie digitali.

In questo scenario la dichiarazione introduce e sviluppa il tema dell'intelligenza artificiale. Questa deve fungere da strumento per le persone con l'obiettivo ultimo di aumentare il benessere umano. La citazione della parola umano è certamente significativa, proprio per la sua collocazione in questo contesto. I concetti esposti si possono riassumere nell'impegno a promuovere sistemi di intelligenza artificiale antropocentrici, affidabili ed etici, garantendo trasparenza funzionale, supervisione umana e gestione della sicurezza tramite meccanismi basati sul rischio.

Questa parte della dichiarazione trova piena applicazione nel regolamento 2024/1689 (AI Act) e grande attenzione si è sviluppata a livello mondiale sul tema. In pratica ci si concentra su aspetti burocratici e formali e appare ancora carente la consapevolezza sull'uso dello strumento in termini di controllo di dati personali o sull'uso non controllato dei motori di intelligenza artificiale generativa da parte del personale delle imprese. Il problema del controllo e gestione dei grandi attori tecnologici è sempre lo stesso, soprattutto sull'uso dei dati e sulle tematiche di influenza sulla popolazione in potenziale violazione dl diritto dell'Unione.

In questo capitolo si tratta anche dell'ambiente digitale equo e della sua fruizione libera da parte delle persone. Le scelte su quali servizi utilizzare devono essere libere e orientate sulla base di informazioni trasparenti e affidabili. La competizione di mercato dovrebbe essere leale e nella direzione dell'innovazione. Le imprese, comprese le PMI dovrebbero avere benefici disponendo, in modo equilibrato dei

giusti spazi di azione e di risorse di supporto.

In Italia questi principi sono stati sviluppati da tempo per le cosiddette startup ma anche per lo stimolo a produrre brevetti. La realtà è rimasta fluida e i grandi successi sono stati spesso raggiunti con finanziamenti esteri, in particolare per i traguardi dei cosiddetti unicorni.

Il CAPITOLO IV dedicato alla partecipazione allo spazio pubblico digitale ne riconosce l'importanza per la democrazia e il dibattito pubblico pluralistico inteso come diritto alla libertà di espressione e di informazione, nonché alla libertà di riunione e di associazione nell'ambiente digitale. La dichiarazione evidenzia la responsabilità delle piattaforme online, specialmente quelle di grandi dimensioni, nel sostenere un dibattito libero, in linea con le regole della democrazia, con il contrasto alla disinformazione.

Su questi diritti e principi non si può che essere ampiamente d'accordo. Il fatto che i social siano parte del gruppo delle "*big tech*" rende deboli queste indicazioni della dichiarazione. Il problema è mondiale e non sono dell'Unione e conseguentemente nazionale e la realtà, spesso, ci porta in direzione opposta a quella della dichiarazione in esame.

Il CAPITOLO V affronta un tema cruciale del mondo digitale, quello della sicurezza e della protezione dei dati personali. Numerose sono le normative comunitarie sul tema ma la loro applicazione è ancora insufficiente.

La dichiarazione afferma che ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali sicuri e protetti, che tutelino la protezione dei dati personali già in fase di progettazione; viene indicato anche l'impegno a contrastare i rischi di cybersecurity e la criminalità informatica.

Il diritto alla protezione dei dati personali non poteva mancare nella Dichiaraziine, sottolineando che ogni persona deve avere il controllo effettivo sui propri dati con la corretta attenzione alla proporzionalità e minimizzazione del trattamento.

Su questi temi non siamo messi bene. Gli attacchi informatici sono numerosi e si concentrano sull'uso del *ransomware* e del DDOS. Gli investimenti in materia di contromisure non sono ancora adeguati. In materia di protezione dei dati personali è evidente la carenza di consapevolezza di cittadini e imprese. Molte sanzioni del Garante per la protezione dei dati personali sono per violazioni ingenue derivanti da scarsa consapevolezza delle regole e conseguente superficialità nell'applicazione, si può sintetizzare con un "non capisco e allora invento".

La protezione di bambini e comunque dei giovani nell'ambiente digitale deve avere una particolare attenzione. L'attrazione ingenua e ludica della rete induce a

comportamenti pericolosi anche per la propria incolumità personale (le tristemente note *challenge* su alcuni social). Questi utenti fragili del mondo digitale devono essere messi in condizione di attuare scelte sicure e informate, essere protetti da contenuti dannosi e illegali, e non essere oggetto di tracciamento e profilazione illeciti.

La società digitale non protegge ancora adeguatamente i soggetti più fragili. Il mondo adulto preparato ad educare a non accettare caramelle dagli sconosciuti non è abbastanza preparato sui pericoli del mondo digitale. Ancora una volta il tema centrale non è quello di fare norme e regole ma quello di educare e rendere consapevoli gli utenti, di qualunque età.

Il CAPITOLO VI è l'ultimo della dichiarazione e affronta l'impatto ambientale della tecnologia digitale, affermando che i prodotti e servizi digitali dovrebbero essere progettati, prodotti e smaltiti in modo da minimizzare l'impatto negativo sull'ambiente, promuovendo l'economia circolare e contrastando l'obsolescenza prematura.

Queste affermazioni sono pienamente condivisibili perché l'inquinamento da microplastiche o il consumo energetico dei grandi data center e di pari importanza a quello del vertiginoso aumento dei rifiuti elettronici. Il mercato crea anche delle situazioni paradossali sull'obsolescenza prematura chiudendo il ciclo di vita di diffusissimi sistemi operativi con la conseguente rottamazione di milioni di personal computer. Il mercato ha sviluppato tecniche di recupero dei materiali obsoleti ma queste attività devono essere a loro volta sostenibili altrimenti la situazione è divergente.

# 3. Conclusioni

Sulla base di quanto esposto possiamo affermare che la dichiarazione rappresenta un impegno politico e una responsabilità condivisa tra l'Unione e gli Stati membri. Pur non introducendo nuove norme giuridiche, specifica come i valori e i diritti fondamentali dell'Unione debbano essere applicati nell'era digitale, introducendo con adeguata azione istituzionale una guida per i responsabili politici e un punto di riferimento per la società.

In un mondo sempre più digitalizzato, questa dichiarazione rappresenta un passo significativo verso un modello europeo di trasformazione digitale che non si concentra solo sull'innovazione tecnologica, ma pone al centro i diritti delle persone e i valori democratici.

In termini di attuazione di questi diritti e principi si può dire che sono attuati in modo quasi completo in modo formale ma sul piano sostanziale ci sono nume-

rose carenze o spazi di miglioramento. La pubblica amministrazione, che fisiologicamente influenza anche gli attori di mercato, mantiene un approccio burocratico, spesso difensivo. Viene data massima attenzione alle regole formali e allo sviluppo di sanzioni. I servizi in rete sono numerosi e di alta efficienza per quanto riguarda le amministrazioni centrali. Lo sviluppo di SPID e del servizio PagoPA è senz'altro rilevante nei rapporti tra pubblica amministrazione e cittadini ed imprese. I servizi fiscali e delle agenzie previdenziali sono un ottimo esempio di operatività dei servizi in rete. La piena attuazione dell'identità digitale europea tramite il Portafoglio di Identità Digitale potrebbe portare ad un nuovo livello di digitalizzazione più diffuso, omogeneo ed equilibrato all'interno dell'Unione.

Negli enti locali molto lavoro è stato fatto con i finanziamenti del PNRR e bisogna attendere gli effetti pratici.

Senza dubbio la parte cybersecurity e protezione dei dati personali è da migliorare con attenzione alla formazione del personale pubblico e privato ma anche dei cittadini. Il problema del furto di identità e delle truffe online è conseguenza del comportamento imprudente dell'utente che favorisce operazioni che nel mondo reale non farebbe mai.

Per l'attuazione della dichiarazione è indispensabile attendere la diffusione dell'identità digitale europea che parte con i giusti principi ed equilibri tecnologici. Un'identità unica a livello europeo, interoperabile e allo stato dell'arte su sicurezza e protezione dei dati personali è rassicurante. Questa base di partenza può portare a conseguenti effetti positivi in quasi tutti i settori trattati nella dichiarazione. Il livello di servizio del mondo digitale deve essere massimo, solo in questo modo la transizione può essere gradita al mondo reale che deve vivere con il giusto equilibrio con quello digitale. La mancanza di questa essenziale premessa ha la conseguenza di un approccio irritato e di mero adempimento verso il digitale e come nella vita delle persone la mancanza di fiducia reciproca non porta a risultati positivi e al benessere della persona auspicato dalla dichiarazione europea sui diritti e i principi digitali.

N. 3 - 2025 - pp. 61-76

# La sostenibilità digitale come elemento abilitante di cittadinanza

**Stefano Epifani - Paolo De Nardis - Matteo Bozzoli**

Il Decennio Digitale Europeo (2021-2030), delineato dalla Commissione Europea attraverso la comunicazione "2030 Digital Compass", mira a costruire un futuro digitale sostenibile, inclusivo e competitivo per l'Europa. Tra gli obiettivi prioritari figurano la promozione delle competenze digitali, la realizzazione di infrastrutture digitali sicure e sostenibili, la digitalizzazione delle imprese e la trasformazione dei servizi pubblici. Questi pilastri sono centrali per una crescita economica equa, resiliente e inclusiva, basata su una solida cultura digitale e su tecnologie orientate al bene comune[1].

In questo quadro europeo, la definizione di una Carta dei Diritti di Internet rappresenta una delle sfide più complesse e rilevanti della contemporaneità. Tale operazione non può esaurirsi nella mera formulazione teorica di principi, ma deve necessariamente tradursi in strumenti concreti di capacitazione dei cittadini, attraverso la promozione di una cultura diffusa della consapevolezza digitale. In un ecosistema sociale sempre più pervaso dalle tecnologie digitali, il riconoscimento formale dei diritti deve essere accompagnato dalla promozione di capacità effettive di comprensione, esercizio critico e difesa di tali diritti. Questo approccio implica la costruzione di un tessuto sociale in grado di interpretare consapevolmente le dinamiche digitali, evitando la marginalizzazione di segmenti della popolazione meno preparati.

In tal senso, l'articolo 3 della Costituzione italiana, che stabilisce che "*è compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese*"[2], costituisce un imprescindibile fondamento teorico e normativo da cui partire per immaginare un'azione coerente nell'ambito della cittadinanza digitale.

---

1 *Commissione Europea, "2030 Digital Compass", 2021*

2 *Costituzione della Repubblica Italiana, art. 3, Gazzetta Ufficiale della Repubblica Italiana, 1948*

La definizione di una Carta dei Diritti di Internet rappresenta una delle sfide cruciali per il consolidamento del Decennio Digitale Europeo. Tale Carta trova un diretto collegamento con il Digital Services Act (DSA) e il Digital Markets Act (DMA), strumenti legislativi europei finalizzati a garantire uno spazio digitale sicuro, equo e competitivo. Il DSA, in particolare, mira a rafforzare la tutela dei diritti fondamentali degli utenti online, regolamentando responsabilità e obblighi delle piattaforme digitali. Integrare i principi della Carta con gli obiettivi del DSA significa assicurare che la digitalizzazione rispetti e promuova diritti fondamentali quali la libertà di espressione, la privacy e l'accessibilità universale ai servizi digitali (Regolamento UE 2022/2065, Digital Services Act).

# 1. La sostenibilità digitale come paradigma per l'esercizio dei diritti

Alla luce di queste considerazioni, emerge con forza l'urgenza di disporre di strumenti idonei a misurare e analizzare il livello di consapevolezza, competenze e comportamenti digitali della popolazione. Come indicato nel "Manifesto per la Sostenibilità Digitale" della Fondazione per la Sostenibilità Digitale[3], la sostenibilità digitale è concettualizzata non solo come minimizzazione degli impatti ambientali delle tecnologie, ma anche come uso consapevole e responsabile delle stesse quale leva sistemica per uno sviluppo socio-economico equo, inclusivo e resiliente. Questo paradigma riconosce nel digitale non solo un ambito di trasformazione tecnica, ma un terreno su cui si giocano sfide culturali, economiche e sociali decisive.

La sostenibilità digitale, come definita nel "Manifesto per la Sostenibilità Digitale", si integra coerentemente negli obiettivi della transizione gemella ("twin transition") promossa dall'Unione Europea. Tale approccio mira a combinare la trasformazione digitale e la transizione ecologica, due sfide intrinsecamente connesse e complementari. La sostenibilità digitale supera dunque la semplice minimizzazione degli impatti ambientali delle tecnologie, promuovendo un uso consapevole e responsabile del digitale quale leva strategica per un progresso socioeconomico equo, inclusivo e resiliente. Questo paradigma europeo riconosce nel digitale un fondamentale acceleratore per raggiungere gli obiettivi del Green Deal, integrando innovazione tecnologica, giustizia sociale e sostenibilità ambientale[4].

La digitalizzazione e la trasformazione digitale, infatti, pur essendo strettamente

[3] *Fondazione per la Sostenibilità Digitale, Manifesto per la Sostenibilità Digitale, 2021*

[4] Commissione Europea, Comunicazione "Il Green Deal Europeo e la Transizione Digitale", 2020

interconnesse, rappresentano fenomeni concettualmente e operativamente distinti. La digitalizzazione concerne l'automazione dell'informazione e la trasposizione dei processi analogici in formati digitali, con l'obiettivo primario di incrementare l'efficienza, la precisione e la velocità operativa. Essa si focalizza sul "come" svolgiamo le nostre attività quotidiane: dalla gestione documentale alla comunicazione organizzativa. La digitalizzazione rappresenta una fase evolutiva necessaria, ma limitata, poiché si concentra prevalentemente sull'ottimizzazione di processi esistenti senza necessariamente mutare in profondità le strutture sociali ed economiche.

La trasformazione digitale, invece, si presenta come un fenomeno strutturale e irreversibile che investe l'intero ecosistema sociale. Essa ridefinisce radicalmente le dinamiche economiche, sociali e culturali, modificando profondamente i significati attribuiti alle attività umane. La trasformazione digitale è un "*fenomeno sistemico in grado di modificare non solo i processi, ma gli stessi modelli cognitivi, le aspettative sociali e le forme della produzione e del consumo*"[5].
Questo carattere pervasivo implica che essa debba essere affrontata come fenomeno eminentemente sociale e culturale, richiedendo approcci sistemici e multidisciplinari.

La trasformazione digitale si configura quindi come un processo di evoluzione sistemica che, pur scaturendo da scelte tecnologiche, economiche e sociali, una volta avviato acquisisce una dinamica autonoma che ne rende complessa la gestione e l'indirizzamento. Non può essere orientata arbitrariamente, né modellata secondo volontà contingenti, in quanto - come sottolinea Lessig - nel digitale "*il codice è legge*"[6], poiché è determinata da interazioni stratificate tra innovazione tecnologica, modelli di business, normatività sociale e aspettative culturali. Tuttavia, è possibile indirizzare il suo sviluppo attraverso un approccio sistemico che sappia riconoscere, interpretare e intervenire sulle interconnessioni tra le diverse dimensioni coinvolte. In tale prospettiva, la direzione non è imposta bensì co-costruita, frutto di strategie capaci di integrare tecnologia, etica, economia e politica in un quadro coerente e orientato a obiettivi condivisi. La sfida è dunque quella di adottare strumenti e metodologie che permettano di leggere la complessità della trasformazione digitale e di intervenire su di essa non attraverso regolazioni settoriali o interventi isolati, ma mediante politiche pubbliche, pratiche organizzative e iniziative sociali capaci di promuovere traiettorie di sviluppo compatibili con principi di equità, inclusione e resilienza.

In questo contesto, una risposta solida e sistemica può essere offerta da un approccio fondato sulla sostenibilità, evitando le illusioni digitali di liberazione automatica

---

[5] Stefano Epifani, Sostenibilità Digitale: perché la sostenibilità non può fare a meno della trasformazione digitale (Roma: Digital Transformation Institute, 2020)

[6] *Lawrence Lessig, Code and Other Laws of Cyberspace (New York: Basic Books, 1999)*

denunciate da Morozov[7]. Intesa nella sua accezione più piena — che integra le dimensioni ambientale, economica e sociale — la sostenibilità fornisce non solo una cornice di valori, ma anche criteri operativi per orientare il cambiamento. Adottando la sostenibilità come principio guida è possibile garantire che la trasformazione digitale non diventi fattore di nuova marginalizzazione, ma si traduca in un motore di innovazione responsabile, capace di promuovere uno sviluppo realmente umano e duraturo.

Nel quadro della cittadinanza digitale, l'esercizio effettivo dei diritti non dipende più soltanto dalla loro enunciazione formale ma riflette, come afferma Sassen, una rinegoziazione dei diritti nell'era globale[8] che rappresenta la capacità collettiva di creare contesti in cui lo sviluppo tecnologico sia orientato ai principi della sostenibilità. In assenza di tale prospettiva, la trasformazione digitale rischia di amplificare disuguaglianze, precarietà occupazionale e crisi ambientali, come avvertito da Zuboff nel suo studio sul capitalismo della sorveglianza[9], esacerbando le vulnerabilità preesistenti. Pertanto, la sostenibilità emerge come faro normativo imprescindibile da integrare nelle politiche di governance di Internet[10], come sostiene Mueller, capace di indirizzare l'innovazione tecnologica verso obiettivi di equità, inclusione e responsabilità intergenerazionale. In questa prospettiva, si rende necessario dotarsi di strumenti capaci di misurare e interpretare il livello di consapevolezza, competenza e comportamento dei cittadini rispetto alla trasformazione digitale, al fine di tradurre i principi della sostenibilità in pratiche concrete e orientare efficacemente le politiche pubbliche e le strategie di innovazione.

In questo contesto, la sostenibilità digitale è intesa come "*il ruolo sistemico del digitale rispetto alla sostenibilità, guardando ad esso da una parte come strumento di supporto per il perseguimento degli obiettivi di sviluppo sostenibile, dall'altra come elemento da indirizzare attraverso criteri di sostenibilità. In questo duplice ruolo, la sostenibilità digitale riguarda quindi le interazioni della digitalizzazione e della trasformazione digitale rispetto a sostenibilità ambientale, economica e sociale*". Essa si configura quindi come un elemento cardine per la costruzione di una società digitale in cui le opportunità offerte dalle tecnologie siano pienamente orientate al bene comune[11] e alla promozione di modelli di sviluppo sostenibili, inclusivi e resilienti. Rappresenta il paradigma attraverso cui interpretare le profonde interrelazioni

---

7 *Evgeny Morozov, The Net Delusion: The Dark Side of Internet Freedom (New York: PublicAffairs, 2011)*

8 *Saskia Sassen,* Territory, Authority, Rights *(Princeton: Princeton University Press, 2006)*

9 *Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019)*

10 Milton Mueller, *Networks and States: The Global Politics of Internet Governance* (Cambridge, MA: MIT Press, 2010)

11 *Byron Reese,* The Fourth Age: Smart Robots, Conscious Computers, and the Future of Humanity *(New York: Atria Books, 2018)*

tra dimensioni ambientali, economiche e sociali e, allo stesso tempo, uno strumento operativo che consente di governare il cambiamento tecnologico in modo consapevole e responsabile. In sostanza, la sostenibilità digitale si configura come un presupposto fondamentale per garantire l'esercizio effettivo dei propri diritti nella società digitale e per dare piena attuazione ai principi sanciti in una Carta dei Diritti di Interne che voglia produrre un cambiamento reale nella società. La sostenibilità digitale, infatti, consente non solo di accedere alle opportunità offerte dalla trasformazione tecnologica, ma anche di farlo in modo critico, consapevole e responsabile, preservando i valori fondamentali di equità, inclusione, libertà e rispetto della dignità umana. Qualsiasi Carta dei Diritti di Internet, per essere realmente efficace, richiede infatti cittadini capaci di comprendere, esercitare e difendere i propri diritti nell'ecosistema digitale, nella prospettiva di Internet come bene pubblico come proposto da Berners-Lee[12], evitando che l'accesso alle tecnologie si traduca in nuove forme di disuguaglianza o esclusione. Attraverso un uso sostenibile del digitale, i cittadini possono esercitare pienamente la loro capacità di autodeterminazione, come evidenziato da Benkler nel sottolineare il ruolo delle reti distribuite nella produzione di beni comuni[13], partecipare attivamente alla vita democratica, vigilare sull'uso etico delle tecnologie e contribuire alla costruzione di un ecosistema digitale orientato al bene comune e alla sostenibilità delle generazioni future.

Alla luce di ciò, emerge con chiarezza che la costruzione di una società digitale sostenibile e inclusiva richiede non solo la definizione di diritti formali, ma anche la capacità di verificarne l'attuazione concreta attraverso strumenti di misurazione adeguati. Misurare il livello di consapevolezza, competenza e comportamento dei cittadini è un passaggio essenziale per comprendere in che misura la popolazione sia realmente in grado di esercitare i propri diritti nell'ecosistema digitale. Solo attraverso un'analisi sistematica e rigorosa di queste dimensioni è possibile individuare le aree di fragilità culturale, progettare interventi mirati di alfabetizzazione digitale e promuovere politiche pubbliche in grado di ridurre il divario digitale. In questo senso, la misurazione non rappresenta un fine in sé, ma uno strumento operativo imprescindibile per tradurre i principi della sostenibilità digitale in pratiche effettive, orientando consapevolmente il processo di trasformazione tecnologica verso obiettivi di equità, inclusione e resilienza.

---

[12] *Tim Berners-Lee, Weaving the Web (San Francisco: Harper, 1999)*

[13] *Yochai Benkler, The Wealth of Networks (New Haven: Yale University Press, 2006)*

# 2. L'osservatorio per la Sostenibilità Digitale e il Digital Sustainbility Index (DiSI)

In risposta alla necessità di disporre di strumenti capaci di misurare e interpretare il livello di consapevolezza, competenza e comportamento dei cittadini rispetto alla trasformazione digitale, la Fondazione per la Sostenibilità Digitale, in collaborazione con l'Istituto di Studi Politici San Pio V, ha avviato nel 2020 l'Osservatorio per la Sostenibilità Digitale. L'Osservatorio raccoglie, analizza e interpreta dati utili a comprendere come il digitale incida sui processi di sostenibilità ambientale, sociale ed economica.

Esso analizza il livello di percezione degli Italiani rispetto a tre dimensioni fondamentali:

- **Consapevolezza**: rappresenta la comprensione critica del ruolo sistemico delle tecnologie digitali, includendo la capacità di riconoscerne le implicazioni etiche, sociali ed economiche. Non si tratta soltanto di conoscere gli strumenti digitali, ma di interpretare il loro impatto sulla società nel suo complesso, considerando le conseguenze culturali, ambientali e democratiche di ogni innovazione tecnologica. Una consapevolezza matura implica la capacità di valutare criticamente i modelli economici sottesi all'innovazione digitale e di contribuire attivamente alla definizione di un ecosistema tecnologico più equo e sostenibile.
- **Competenze**: comprendono l'insieme delle abilità operative e cognitive necessarie per un utilizzo sostenibile e consapevole delle tecnologie. Esse includono sia le capacità tecniche (alfabetizzazione digitale, gestione sicura dei dati, utilizzo responsabile delle piattaforme) sia quelle critiche e strategiche (valutazione delle fonti informative, comprensione degli algoritmi, protezione dei diritti digitali, promozione dell'accessibilità). Le competenze digitali non si esauriscono nella padronanza tecnica, ma devono integrare la dimensione etica, favorendo comportamenti orientati alla tutela dei diritti umani e al rispetto della diversità culturale.
- **Comportamenti**: costituiscono la traduzione concreta di consapevolezza e competenze in azioni quotidiane coerenti con i principi della sostenibilità. Essi si manifestano attraverso pratiche che promuovono la riduzione dell'impronta ecologica del digitale (ad esempio mediante l'adozione di pratiche di green IT), l'inclusione sociale attraverso l'abbattimento delle barriere digitali e la promozione della parità di accesso, e la difesa attiva dei diritti fondamentali, opponendosi a fenomeni come la discriminazione algoritmica e la sorveglianza di massa.

Il framework di analisi sviluppato ha permesso di ottenere un quadro estrema-

mente articolato e complesso del livello di consapevolezza, delle competenze e dei comportamenti degli italiani rispetto alla trasformazione digitale e alla sostenibilità. Proprio in funzione di tale complessità, si è reso necessario sintetizzare i dati raccolti attraverso la costruzione di un indice di percezione, elaborato dalla Fondazione per la Sostenibilità Digitale, denominato Digital Sustainability Index (DiSI): un indice multidimensionale pensato per misurare il livello di percezione degli italiani rispetto al ruolo della tecnologia come strumento di sostenibilità.

La struttura del DiSI si basa su tre sotto-indici principali:

1. **Indice di digitalizzazione**: misura la percezione da parte degli italiani del grado di diffusione e utilizzo delle tecnologie digitali, analizzando come le persone, le organizzazioni e i territori si sentano digitalmente connessi e quanto ritengano che questo influenzi le loro abitudini quotidiane. Include anche la percezione della presenza di infrastrutture digitali, come l'accesso a internet e la disponibilità di dispositivi tecnologici.
2. **Indice di sostenibilità**: analizza come i cittadini percepiscano il livello di adozione di comportamenti sostenibili nella vita quotidiana e nelle attività produttive, con particolare attenzione alle pratiche che riducono l'impatto ambientale, migliorano l'efficienza delle risorse e promuovono la responsabilità sociale.
3. **Indice di sostenibilità digitale**: misura la percezione degli utenti rispetto all'impatto delle tecnologie digitali sulla sostenibilità ambientale, sociale ed economica, valutando la loro consapevolezza sull'uso delle tecnologie digitali per supportare pratiche sostenibili, come la riduzione dell'impronta ecologica digitale, l'ottimizzazione delle risorse e la promozione dell'inclusione sociale.

Articolando i tre sotto-indici rispetto ai tre ambiti di analisi considerati, il DiSI sviluppa un quadrante interpretativo che suddivide i cittadini in quattro categorie principali, permettendo di comprendere meglio la relazione tra uso delle tecnologie digitali e orientamento verso la sostenibilità:

1. **Sostenibili Digitali**: sono coloro che adottano comportamenti e atteggiamenti sostenibili nei confronti dell'ambiente e della società, e che al contempo utilizzano strumenti digitali in modo consapevole, promuovendo una trasformazione digitale orientata al bene comune.
2. **Sostenibili Analogici**: sono coloro che seguono pratiche e comportamenti sostenibili, ma che non fanno uso delle tecnologie digitali o ne fanno un uso molto limitato, rimanendo ai margini dei processi di trasformazione digitale.
3. **Insostenibili Digitali**: sono gli utenti che, pur facendo ampio uso della tecnologia digitale, non dimostrano consapevolezza riguardo all'impatto ambientale, sociale ed economico delle proprie attività digitali, e che non adottano comportamenti orientati alla sostenibilità.

4. **Insostenibili Analogici**: sono coloro che né utilizzano strumenti digitali né adottano comportamenti o atteggiamenti orientati alla sostenibilità, risultando così doppiamente disallineati rispetto agli obiettivi di una trasformazione digitale sostenibile.

Il DiSI si configura, pertanto, non solo come strumento di analisi, ma come piattaforma interpretativa e progettuale capace di orientare politiche pubbliche, programmi educativi e strategie di innovazione verso un modello di trasformazione digitale realmente sostenibile e inclusivo. È solo attraverso l'integrazione di dimensioni tecnologiche, etiche e civiche che sarà possibile garantire una governance democratica della trasformazione digitale. In quest'ottica, strumenti come il DiSI risultano indispensabili per dare attuazione concreta a principi e diritti sanciti da strumenti come la Carta dei Diritti di Internet, poiché consentono di monitorare e interpretare il reale livello di consapevolezza e competenza della cittadinanza digitale, rendendo così possibile intervenire in modo mirato e sistemico per colmare le disuguaglianze e promuovere una partecipazione effettiva ed equa.

# 3. Il profilo degli italiani

Dalla sua definizione iniziale, l'Osservatorio per la Sostenibilità Digitale ha progressivamente esteso e raffinato l'applicazione del Digital Sustainability Index (DiSI) attraverso una serie di declinazioni specifiche, ciascuna finalizzata ad approfondire diversi aspetti delle dinamiche territoriali, sociali e generazionali relative alla sostenibilità digitale, con l'obiettivo di fornire strumenti di analisi sempre più precisi e operativi per le politiche di innovazione responsabile.

- Nel 2022, il DiSI è stato applicato al contesto delle Regioni italiane, consentendo di tracciare una mappatura dettagliata delle differenze territoriali nella percezione della digitalizzazione e della sostenibilità, e mettendo in evidenza le disomogeneità esistenti tra le diverse realtà locali. Questo primo lavoro ha permesso di individuare le regioni più virtuose e quelle maggiormente in difficoltà, stimolando una riflessione sulle politiche territoriali necessarie.
- Nel 2023, l'indice è stato declinato sulle Città Metropolitane, contesti caratterizzati da una complessità sociale, economica e infrastrutturale ancora più marcata. Questa fase di analisi ha permesso di comprendere come la trasformazione digitale e le pratiche di sostenibilità si manifestino nei grandi poli urbani, evidenziando differenze significative sia tra le città che all'interno di esse.
- Nel 2024, il focus è stato ampliato per analizzare l'intero spettro del contesto urbano, confrontando le dinamiche che caratterizzano i piccolissimi comuni

con quelle delle grandi città metropolitane. Questa prospettiva ha permesso di cogliere le profonde differenze legate alla dimensione territoriale e di evidenziare come la densità demografica, l'accessibilità digitale e le pratiche di sostenibilità varino in funzione della scala urbana.

- Infine, nel 2025, l'indice è stato ulteriormente adattato per esplorare la dimensione generazionale, analizzando come le diverse fasce d'età — dai più giovani agli anziani — si rapportino ai temi della trasformazione digitale e della sostenibilità. Questa analisi ha evidenziato trend intergenerazionali significativi, utili per orientare interventi educativi e politiche pubbliche mirate.

Attraverso queste diverse declinazioni, l'Osservatorio ha arricchito e affinato il quadro interpretativo offerto dal DiSI, trasformandolo in uno strumento sempre più sofisticato e capace di orientare con efficacia le politiche pubbliche, le strategie di innovazione e gli interventi di capacitazione dei cittadini nel contesto della trasformazione digitale e della sostenibilità.

Di seguito sono riportati i risultati principali emersi nel tempo.

## 3.1. Considerazioni generali

## Limitata interiorizzazione degli impatti pratici delle ideologie sostenibili

Sebbene circa il 75% della popolazione riconosca l'urgenza della crisi climatica, persiste una disconnessione significativa tra l'adesione ai principi della sostenibilità e la consapevolezza delle loro implicazioni operative. In particolare, si osserva una debolezza nella capacità di correlare i valori ideologici della sostenibilità alle strategie concrete di gestione economica e sociale. Solamente un terzo dei cittadini dimostra un livello di comprensione sufficiente per cogliere le conseguenze pratiche delle proprie scelte valoriali. Questa frattura culturale segnala una carenza di visione sistemica, in cui la sostenibilità non viene integrata in modelli di gestione delle risorse, ridefinizione economica, innovazione tecnologica e trasformazione sociale. Tale carenza rischia di indebolire la portata effettiva delle politiche di transizione sostenibile, compromettendo la diffusione di comportamenti realmente responsabili.

**Dissociazione tra digitale e sostenibilità: un fenomeno emergente**

Le evidenze empiriche indicano un processo di dissociazione psicologica tra digitale e sostenibilità. Tecnologie emergenti, come l'intelligenza artificiale, la blockchain, i big data, i social media, il cloud computing, la realtà aumentata e virtuale, così come i principi della sostenibilità (in particolare quella sociale), vengono percepiti in modo dicotomico: positivamente in chiave collettiva e astratta, negativamente a livello individuale e quotidiano. Analogamente alla percezione divergente delle

strisce pedonali da parte di pedoni e automobilisti, l'atteggiamento verso il digitale risente del contesto percettivo. Sebbene le tecnologie siano generalmente associate a benefici economici e sociali, emergono sentimenti di paura e diffidenza quando esse incidono su ambiti personali come il lavoro e i diritti civili. Tale dissociazione costituisce un ostacolo alla piena valorizzazione delle potenzialità del digitale come strumento di sostenibilità.

**Il digitale come vettore primario della sostenibilità**

Il digitale si configura come un driver più efficace della sostenibilità rispetto alla sola adesione ideologica. La dichiarazione di intenti ambientali, priva di competenze digitali consolidate, raramente si traduce in comportamenti concreti. Al contrario, la padronanza degli strumenti digitali facilita l'adozione stabile di pratiche sostenibili, anche in assenza di una forte motivazione ideologica. Gli individui sensibili alle tematiche ambientali ma carenti in competenze digitali mostrano una progressiva riduzione dei comportamenti sostenibili. Viceversa, coloro che posseggono tali competenze tendono a consolidare e incrementare pratiche operative virtuose. Ciò evidenzia il ruolo strutturale delle competenze digitali come prerequisito imprescindibile per la diffusione capillare e durevole della sostenibilità nella società contemporanea.

**Commoditizzazione tecnologica e depotenziamento della consapevolezza sostenibile**

La commoditizzazione della tecnologia, intesa come standardizzazione e accessibilità di massa, rischia di neutralizzare il suo potenziale trasformativo in chiave sostenibile. Sebbene la digitalizzazione abbia aperto nuove frontiere nella gestione delle risorse, nella tutela ambientale e nel miglioramento del benessere sociale, il suo assimilarsi a un bene di consumo induce una percezione superficiale e strumentale. Tale fenomeno favorisce approcci a breve termine e riduce la capacità di valutare criticamente gli impatti sistemici, culturali e sociali delle innovazioni tecnologiche. In un contesto di rapida obsolescenza tecnologica, viene trascurata la necessità di un approccio riflessivo che consideri le implicazioni distributive e le disuguaglianze generate. Una sostenibilità autentica richiede infatti una prospettiva di lungo periodo e un uso critico ed equo della tecnologia.

**Radicalismo ambientalista e diffidenza tecnologica: una relazione problematica**

Esiste una correlazione significativa tra l'adozione di posizioni ambientaliste radicali e un atteggiamento di diffidenza, se non di ostilità, nei confronti della tecnologia. L'analisi dei microdati rivela come i soggetti maggiormente impegnati sui temi ecologisti tendano a percepire il digitale non come uno strumento di empowerment, ma come una minaccia. Questa reticenza si manifesta anche nei contesti della sharing economy, dove l'utilizzo di piattaforme digitali, potenzialmente capaci di abilitare modelli di consumo più sostenibili e collaborativi, è spesso rifiutato. Tale fenomeno segnala una frattura culturale che limita la capacità di integrare tecnologia e valori ambientali. Superare questa dicotomia richiede un'evoluzione culturale profonda,

capace di rileggere il digitale come strumento abilitante di sostenibilità e non come elemento estraneo o antagonista.

## 3.2. Considerazioni legate alla dimensione urbana
## Dalla dicotomia Nord-Sud alla variabile dimensionale: un nuovo paradigma interpretativo

L'analisi dei dati riferiti alle città italiane suggerisce che la principale linea di frattura socio-culturale non risiede tanto nell'asse Nord-Sud, quanto piuttosto nella dicotomia tra grandi e piccoli centri. Consapevolezza, competenze e comportamenti relativi alla sostenibilità e al digitale risultano essere fortemente correlati alla dimensione demografica dei comuni, più che alla loro collocazione geografica. Grandi agglomerati urbani, come Roma, Milano, Napoli e Palermo, manifestano tratti comportamentali più simili tra loro rispetto a quanto avvenga con i comuni minori della stessa regione. Tale fenomeno si acuisce laddove il divario demografico tra il centro urbano principale e i comuni circostanti si presenta più marcato, riflettendo una diseguaglianza nell'accesso alle risorse e nella partecipazione alla cultura digitale.

**Sostenibilità: una nozione ancora periferica nei piccoli centri**

La diffusione del concetto di sostenibilità, pur in crescita, evidenzia ancora marcate disomogeneità territoriali. Sebbene una parte della popolazione italiana dichiari familiarità con il termine, la percentuale di coloro che ne possiedono una comprensione articolata e profonda rimane marginale. Tale limitazione conoscitiva si manifesta con particolare evidenza nelle aree periferiche e nei piccoli centri urbani, dove oltre la metà degli abitanti dichiara una conoscenza nulla o superficiale del concetto. Questa lacuna non solo ostacola l'adozione di pratiche sostenibili, ma compromette anche l'efficacia degli interventi istituzionali volti alla promozione della sostenibilità, rappresentando una barriera significativa alla costruzione di una cultura condivisa capace di rispondere consapevolmente alle sfide ambientali, sociali ed economiche globali.

**Atteggiamenti verso il digitale: apertura critica nei grandi centri, approccio riflessivo nei piccoli**

Nei grandi centri urbani, l'approccio verso la tecnologia si connota per una generale apertura, associata tuttavia a un atteggiamento più critico rispetto ai piccoli centri. Sebbene la tecnologia venga largamente percepita come opportunità, nei contesti metropolitani si registra una consapevolezza maggiore dei rischi correlati. Paradossalmente, mentre i cittadini dei piccoli comuni si mostrano più riflessivi circa l'assenza di rischi percepiti, emergono evidenze – come nel caso della conoscenza dei deep fake – che indicano una maggiore consapevolezza nei piccoli centri su specifiche problematiche tecnologiche. Questo dato sottolinea l'urgenza di interventi di educazione digitale orientati a rafforzare una comprensione critica e trasversale dei rischi associati alle nuove tecnologie.

**Digitalizzazione della PA: un divario persistente tra centri grandi e piccoli**

L'adozione degli strumenti digitali da parte della Pubblica Amministrazione italiana rivela profonde disparità tra grandi e piccoli centri. Mentre nei primi l'utilizzo di strumenti come SPID, CIE/CNS e PagoPA risulta elevato, nei piccoli comuni tali tecnologie registrano una penetrazione significativamente inferiore. Una parziale eccezione si osserva nel Nord-Est, dove i livelli di adozione si mantengono più bassi anche nei grandi centri. La diseguaglianza nell'accesso e nell'utilizzo delle tecnologie digitali pubbliche rappresenta un ostacolo strutturale alla piena attuazione di politiche di inclusione e innovazione amministrativa.

**Percezione dei rischi tecnologici: una preoccupazione più marcata nei piccoli centri**

Nonostante la riconosciuta potenzialità innovativa della tecnologia, tra la popolazione italiana – e in particolare nei piccoli centri – permane una forte preoccupazione circa le sue implicazioni sociali ed economiche. Il timore di un aumento delle diseguaglianze, della disoccupazione tecnologica e dell'ingiustizia economica si configura come un sentimento diffuso, più accentuato nelle aree meno urbanizzate. Questa percezione critica si estende alla visione della digitalizzazione come possibile ostacolo allo sviluppo sostenibile, evidenziando la necessità di politiche che sappiano conciliare innovazione tecnologica e coesione sociale.

**Privacy e protezione dei dati: un divario di consapevolezza tra grandi e piccoli centri**

La tutela della privacy si conferma una delle principali preoccupazioni dell'era digitale[14], ma la sensibilità verso questo tema varia significativamente a seconda del contesto territoriale. Nei grandi centri urbani si riscontra una maggiore attenzione nella gestione delle informazioni personali, mentre nei piccoli comuni la consapevolezza dei rischi associati alla condivisione online appare più limitata. Quasi il 70% dei residenti nei piccoli centri manifesta una riflessione insufficiente sulle implicazioni della privacy, indicando un'esigenza urgente di rafforzare l'educazione digitale orientata alla protezione dei dati personali, quale prerequisito essenziale per una cittadinanza digitale pienamente consapevole.

[14] *Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford: Stanford University Press, 2010)*

## 3.3. Considerazioni legate alla dimensione generazionale
## Due mondi a confronto: giovani Sostenibili Digitali, anziani Insostenibili Analogici

L'analisi intergenerazionale evidenzia un divario strutturale nell'adozione delle tecnologie digitali e nella propensione verso la sostenibilità ambientale. Le coorti più giovani, in particolare i nati tra il 1981 e il 2012 (Millennials e Generazione Z), si configurano come "Sostenibili Digitali", dimostrando un'elevata digitalizzazione congiunta a una maggiore sensibilità ecologica. Tra i membri della Generazione Z, circa la metà si riconosce in questo paradigma, con i Millennials che, pur in misura inferiore, seguono una traiettoria analoga. Di contro, la Generazione X e i Baby Boomers si caratterizzano prevalentemente come "Insostenibili Analogici", denotando un basso livello di alfabetizzazione digitale e un limitato impegno verso pratiche sostenibili. L'analisi evidenzia una chiara frattura generazionale, con i Baby Boomers che si identificano quasi unanimemente in quest'ultima categoria.

**Digitale: spaventa di più i Baby Boomers, che però, nel tempo libero, lo usano come i più giovani**

Sebbene l'accettazione delle tecnologie digitali sia ormai diffusa tra gli italiani di età compresa tra i 18 e i 60 anni, gli over 60 manifestano ancora elevati livelli di timore rispetto alle potenziali derive negative. Tuttavia, in un'analisi più approfondita degli effetti del digitale su economia e società, circa la metà degli intervistati riconosce nella trasformazione tecnologica un fattore di incremento delle disuguaglianze e della precarizzazione lavorativa. L'utilizzo degli strumenti digitali permane fortemente ludico-ricreativo, e i Baby Boomers, pur utilizzando meno frequentemente tali strumenti rispetto ai più giovani, li adottano prevalentemente in contesti extra-professionali. Le competenze digitali percepite decrescono proporzionalmente all'aumentare dell'età, ma anche tra i Millennials e la Generazione X la percentuale di competenze certificate rimane bassa.

**Tecnologia per la sostenibilità: Non serve per un italiano su quattro, indipendentemente dall'età**

Sebbene esistano evidenti differenze generazionali nell'adozione delle tecnologie, il livello di fiducia nella loro capacità di favorire la sostenibilità si presenta relativamente uniforme: circa un quarto della popolazione italiana, a prescindere dall'età, non riconosce alla tecnologia digitale un ruolo significativo nella promozione della sostenibilità. Solo una minoranza manifesta una convinzione decisa circa il potenziale trasformativo del digitale. I Millennials emergono come il gruppo più critico, mostrando un livello di scetticismo superiore rispetto agli altri segmenti generazionali. Questo scenario suggerisce che le strategie di promozione della sostenibilità digitale debbano essere ripensate in modo da superare le barriere percettive condivise trasversalmente dalle diverse generazioni.

**Sostenibilità: approfondendo, l'età non conta così tanto**
Il livello di familiarità dichiarato con il concetto di sostenibilità varia significativamente tra le generazioni: la Generazione Z si dichiara più informata rispetto ai Baby Boomers, tra i quali una consistente minoranza ammette una conoscenza nulla o superficiale del tema. Tuttavia, analizzando la capacità di tradurre l'ideologia della sostenibilità in comportamenti concreti, si osserva una convergenza intergenerazionale: meno di un terzo degli italiani, indipendentemente dall'età, riesce a collegare la propria visione ideologica con implicazioni pratiche. Analogamente, variabili sociodemografiche come genere e reddito non mostrano effetti differenziali significativi, indicando una carenza cognitiva trasversale.

# 4. Conclusioni

L'analisi condotta attraverso il Digital Sustainability Index (DiSI) evidenzia una frattura significativa tra la crescente consapevolezza dei cittadini italiani riguardo alla sostenibilità e la capacità di tradurre tale consapevolezza in pratiche concrete, specialmente nell'ambito digitale. Questa discrepanza si inserisce in un contesto globale in cui emergono iniziative volte a garantire i diritti fondamentali nell'ambiente digitale.

A livello internazionale, il Global Digital Compact[15] adottato dalle Nazioni Unite nel settembre 2024 rappresenta un passo significativo verso la definizione di principi condivisi per un ambiente digitale responsabile e inclusivo. Il Compact sottolinea l'importanza di garantire l'accesso universale a Internet, proteggere i diritti umani online e promuovere una governance etica dell'intelligenza artificiale. Questi obiettivi rispecchiano le esigenze evidenziate dal DiSI, che mette in luce la necessità di competenze operative per integrare la sostenibilità nella gestione quotidiana delle tecnologie digitali.

In Europa, l'entrata in vigore del Digital Services Act (DSA) nel novembre 2022 ha introdotto nuove regole per le piattaforme online, mirate a prevenire attività illegali e dannose, garantire la sicurezza degli utenti e proteggere i diritti fondamentali. Questa regolamentazione si allinea con le preoccupazioni emerse dal DiSI riguardo alla percezione ambivalente delle tecnologie digitali e alla necessità di una cultura della sostenibilità digitale.

[15] United Nations, *Global Digital Compact*, adottato nel Summit of the Future, settembre 2024.

Negli Stati Uniti, l'approvazione del Global Internet Freedom Act[16] e del Protecting Americans' Data from Foreign Adversaries Act[17] nel 2024 evidenzia l'impegno nel promuovere la libertà di Internet e proteggere i dati sensibili dei cittadini. Queste iniziative legislative rispondono alla crescente preoccupazione per la sicurezza digitale e la protezione dei diritti individuali nell'ambiente online, temi che trovano eco nei risultati del DiSI.

Tuttavia, nonostante questi progressi normativi, il rapporto "Freedom on the Net 2024" di Freedom House[18] segnala un continuo declino della libertà di Internet a livello globale, con condizioni peggiorate in 27 dei 72 paesi analizzati. Questo trend sottolinea l'urgenza di implementare efficacemente le politiche esistenti e di sviluppare ulteriori strategie per garantire un ambiente digitale sicuro e inclusivo.

In sintesi, il percorso evolutivo del DiSI, intrecciato con le recenti iniziative internazionali quali il Global Digital Compact delle Nazioni Unite, il Digital Services Act europeo e le nuove normative statunitensi sulla libertà di Internet e la protezione dei dati, evidenzia con forza una verità ineludibile: sostenibilità e digitalizzazione non possono più essere pensate come ambiti separati, ma devono essere integrati in una cornice comune di diritti, competenze e responsabilità.

Dal punto di vista accademico, emerge la necessità di abbandonare approcci settoriali, che trattano sostenibilità, tecnologia e diritti digitali come compartimenti stagni. È invece indispensabile adottare una prospettiva transdisciplinare, capace di tenere insieme l'alfabetizzazione tecnologica, la consapevolezza ambientale e il rispetto dei diritti umani nell'ambiente digitale. I dati del DiSI confermano infatti che l'acquisizione di competenze digitali rappresenta un prerequisito strutturale non solo per la partecipazione attiva nella società contemporanea, ma anche per l'attuazione concreta dei principi di sostenibilità, così come richiesto dai più recenti modelli di sviluppo umano integrato promossi da organismi internazionali come l'ONU.

Nel quadro del Decennio Digitale Europeo, la sostenibilità digitale diventa un principio cardine, una bussola strategica per orientare l'Europa verso obiettivi ambiziosi e imprescindibili: la neutralità climatica entro il 2050, una società digitale inclusiva, e la costruzione di economie resilienti capaci di affrontare sfide globali come quelle ambientali, sociali ed economiche. La visione europea per il 2030 non concepisce la digitalizzazione soltanto come progresso tecnologico, ma come una rivoluzione culturale e sociale, necessaria per garantire coesione, equità e sostenibilità intergenerazionale. Affinché tale visione diventi realtà, sarà essenziale promuovere competenze digitali diffuse, una cultura della responsabilità e strumenti efficaci di

[16] United States Congress, *Global Internet Freedom Act* (H.R.8309), approvato nel 2024

[17] United States Congress, *Protecting Americans' Data from Foreign Adversaries Act*, 2024

[18] Freedom House, *Freedom on the Net 2024: The Repressive Power of Artificial Intelligence*, 2024

governance partecipata, trasformando così il digitale in un patrimonio comune e sostenibile, capace di affrontare le sfide del nostro tempo e di assicurare una prosperità autenticamente inclusiva e duratura[19].

L'integrazione fra diritti digitali e sostenibilità impone inoltre un ripensamento radicale delle strategie educative e delle politiche pubbliche. Non basta più garantire l'accesso alle tecnologie: occorre costruire cittadinanze digitali consapevoli, capaci di utilizzare gli strumenti digitali non solo per finalità ludiche o consumistiche, ma come leve di emancipazione individuale e collettiva, in linea con quanto auspicato dalla Dichiarazione dei diritti in Internet italiana e ribadito a livello internazionale.

Ma al di là dell'analisi tecnico-accademica, serve una visione. Occorre immaginare il digitale non come una semplice infrastruttura tecnologica, ma come l'ecosistema primario della cittadinanza del XXI secolo: un habitat sociale, economico e culturale dove si giocano non solo le opportunità di crescita e innovazione, ma anche le fondamenta della giustizia, dell'equità e della sostenibilità futura. La costruzione di una sostenibilità digitale integrale diventa così la sfida epocale del nostro tempo: una sfida che richiede coraggio istituzionale, creatività pedagogica, responsabilità politica e impegno etico trasversale.

In un mondo in cui la libertà di espressione online è minacciata, la privacy personale è costantemente sotto attacco, e la disuguaglianza di accesso alle risorse digitali si amplifica, non possiamo permetterci di trattare la sostenibilità digitale come un'opzione accessoria. Essa è, oggi più che mai, il presupposto ineliminabile per la sopravvivenza democratica e per la realizzazione di un futuro che sia davvero a misura d'uomo e di pianeta.

È necessario agire ora, affinché il digitale non diventi strumento di nuove esclusioni o nuove disuguaglianze, ma invece si configuri come una infrastruttura comune di diritti, un terreno di inclusione sociale e una leva di rigenerazione planetaria. In questa prospettiva, la sostenibilità digitale non è solo un ambito di studio o una direzione di policy: è il cuore stesso di una nuova promessa di civiltà.

[19] Dichiarazione di Lisbona sul Decennio Digitale Europeo, 2021

N. 3 - 2025 - pp. 77-82

# Gli USA inventano, la Cina copia e l'Europa norma...

**Enzo Chilelli**

**Abstact:** Con questo titolo scherzoso, ma non troppo, iniziamo questo articolo sulla dichiarazione europea sui diritti e i principi digitali tesa a promuove una transizione digitale che rispetti i valori europei al fine di consentire ai cittadini di godere appieno delle opportunità offerte dalla transizione digitale. La dichiarazione comprende anche l'impegno dell'UE e degli Stati membri ad **agire** in una serie di questioni digitali.

With this jokey, but not too much, title, we begin this article on the European declaration on digital rights and principles aimed at promoting a digital transition that respects European values in order to allow citizens to fully enjoy the opportunities offered by the digital transition. The declaration also includes a commitment from the EU and its member states to take action on a range of digital issues.

## Introduzione

Basata sulla Carta dei diritti fondamentali dell'UE, la dichiarazione ricorda i diritti più importanti nella trasformazione digitale, quali la libertà di espressione e di informazione, la protezione dei dati e la vita privata.
I principi sono strutturati intorno a 6 temi:

### 1. Mettere le persone e i loro diritti al centro della trasformazione digitale

La tecnologia dovrebbe servire e giovare a tutte le persone che vivono nell'UE e consentire loro di perseguire le proprie aspirazioni. Non dovrebbe violare la loro sicurezza o i loro diritti fondamentali.

L'UE e i suoi Stati membri si impegnano a garantire che la trasformazione digitale vada a vantaggio di tutti e migliori la vita di tutte le persone che vivono nell'UE. Adottano misure per garantire che i nostri diritti siano rispettati sia online che offline e promuovono questo approccio sia a casa che sulla scena internazionale.

## 2. Sostenere la solidarietà e l'inclusione

L'accesso universale a una tecnologia inclusiva che rispetti i diritti dell'UE è essenziale. Tutti dovrebbero:

- avere accesso a **una connettività** digitale a prezzi accessibili e ad alta velocità
- essere in grado di acquisire l'istruzione **e le competenze** necessarie per godere dei benefici della tecnologia digitale
- avere **condizioni di lavoro eque e giuste**
- avere accesso ai **principali servizi pubblici digitali**

L'UE e i suoi Stati membri si sono impegnati a non lasciare indietro nessuno, sostenendo gli sforzi volti a dotare tutti gli istituti di istruzione e formazione, garantendo il diritto alla disconnessione dal lavoro e fornendo un'identità digitale che dia accesso a un'ampia gamma di servizi online.

## 3. Garantire la libertà di scelta online

Ognuno dovrebbe avere il potere di fare le proprie scelte informate online. Ciò include l'interazione con i sistemi di intelligenza artificiale, che dovrebbero fungere da strumento per le persone, con l'obiettivo ultimo di aumentare il benessere umano.

L'UE e gli Stati membri si impegnano in particolare a promuovere sistemi di intelligenza artificiale antropocentrici, affidabili ed etici, utilizzati in modo trasparente e in linea con i valori dell'UE.

La libertà di scelta include anche la libertà di scegliere quali servizi online utilizzare, sulla base di informazioni oggettive, trasparenti e affidabili. Questo a sua volta implica assicurarsi che le aziende abbiano il potere di competere e innovare nel mondo digitale.

## 4. Promuovere la partecipazione allo spazio pubblico digitale

Tutti dovrebbero avere accesso a un ambiente online affidabile, diversificato e multilingue e dovrebbero sapere chi possiede o controlla i servizi che stanno utilizzando. Ciò incoraggia il dibattito pubblico pluralistico e la partecipazione alla democrazia.

La dichiarazione sottolinea inoltre la necessità di creare un ambiente digitale che protegga le persone dalla disinformazione, dalla manipolazione delle informazioni e da altre forme di contenuti dannosi, comprese le molestie e la violenza di genere.

Riconosce il ruolo delle piattaforme online di dimensioni molto grandi in tale contesto e chiede loro di attenuare i rischi derivanti dal funzionamento e dall'uso dei loro servizi.

L'UE e gli Stati membri si impegnano in particolare a sostenere un accesso effettivo ai contenuti digitali che rifletta la diversità culturale e linguistica nell'UE.

## 5. Aumentare la sicurezza e l'emancipazione delle persone (soprattutto dei giovani)

Tutti dovrebbero avere accesso a tecnologie, prodotti e servizi digitali sicuri e protetti dalla vita privata. L'UE e gli Stati membri si impegnano in particolare a proteggere gli interessi delle persone, delle imprese e dei servizi pubblici dalla criminalità informatica e a garantire che tutti abbiano un controllo effettivo sui propri dati personali e non personali in linea con il diritto dell'UE.

I bambini e i giovani dovrebbero avere la possibilità di compiere scelte sicure e informate ed esprimere la loro creatività nell'ambiente digitale. L'UE e gli Stati membri si impegnano inoltre a promuovere esperienze positive per i bambini e i giovani in un ambiente digitale sicuro e adeguato all'età e a proteggerli dai contenuti dannosi e illegali, dallo sfruttamento, dalla manipolazione e dagli abusi online.

## 6. Promuovere la sostenibilità del futuro digitale

Le transizioni digitale e verde sono strettamente collegate. Sebbene le tecnologie digitali offrano molte soluzioni ai cambiamenti climatici, dobbiamo assicurarci che non contribuiscano da sole al problema. I prodotti e i servizi digitali dovrebbero essere progettati, prodotti e smaltiti in modo sostenibile.

L'UE e gli Stati membri si impegnano a sostenere le tecnologie digitali con effetti ambientali e sociali negativi minimi. L'obiettivo è promuovere le tecnologie digitali che hanno un impatto positivo sull'ambiente e sul clima, contribuendo alla transizione verde. Si impegnano inoltre a promuovere standard e marchi di sostenibilità per prodotti e servizi digitali, per fornire alle persone maggiori informazioni sul loro impatto ambientale.

La dichiarazione europea sui diritti e i principi digitali offre ai cittadini un ponte verso le leggi e le politiche digitali dell'Unione, in quanto indica la direzione di marcia dell'Unione nel suo cammino verso la trasformazione digitale.

# Tutti principi sacrosanti ma l'attuazione?

Siamo stati tra i primi Paesi al mondo, nel 2004, a dotarci di una normativa specifica sul digitale, limitata, per scelta, al settore pubblico, il Codice dell'Amministrazione Digitale i cui principi sono stati posti alla base di molti atti europei fino al Next Generation EU o PNRR, come sbagliando viene più comunemente chiamato qui da noi.

Tutti atti che indicano imprese, cittadini, famiglie, e giovani generazioni come i veri detentori del potere, ma è proprio così? Già oggi quei saggi principi enunciati sono spesso disattesi, trincerandosi dietro altre norme e prassi che poco o nulla hanno a che fare con gli enunciati. Di seguito sintetizzo quelli che reputo maggiormente significativi:

1) **razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese**
2) **le PA utilizzano esclusivamente i canali e i servizi telematici**
3) **Digital first, tutto nella PA nasce in formato digitale.**
4) **Once only, la PA chiede un dato una sola volta al cittadino e se una PA ha bisogno di informazioni che detiene un altra PA, non usa il cittadino come garzone per il trasferimento del documento, ma i dati vengono scambiati tramite interoperabilità applicativa.**
5) **Cloud first, i servizi delle PA sono gestiti nativamente su servizi cloud.**
6) **Interoperabile by design, le PA, nella realizzazione di piattaforme applicative, pensano all'interoperabilità dei software e delle banche dati, per lo scambio dati tra lo stesso ente o tra enti diversi.**
7) ***Sostenibili, uso di* risorse certe da gestire in modo trasparente e con le dovute coperture;**
8) **Riuso: qualsiasi investimento di una PA è messo a fattor comune delle altre amministrazioni e della collettività.**

È facile sorridere ad ogni punto enunciato pensando ai nostri calvari nl rapporto con le PA. Ma presumo che ciò non migliorerà a breve, oggi le bigtech fatturano più di molti Stati (compreso il nostro) e riescono ad indirizzare anche le politiche.

L'avvicinarsi della 5^ rivoluzione industriale, quella che deriverà dall'uso pervasivo dell'intelligenza artificiale, che noi abbiamo "normato" e che il nuovo presidente USA ha liberato da ogni vincolo al fin di garantire la perpetuazione dl primato tecnologico statunitense, difficilmente garantirà quel livello di "democrazia" descritto nelle norme e negli atti di indirizzo.

Il dibattito sulla sovranità digitale è aperto da anni, da un lato, emerge come

risposta alla crescente dipendenza tecnologica dell'UE da fornitori esterni, in particolare USA e Cina. Dall'altro, diversi esperti sostengono che una vera sovranità digitale sia impossibile senza la collaborazione con i grandi player tecnologici. Realtà entrambi reali allo stato delle cose.

I dati sono rivelatori: attualmente, una percentuale impressionante – oltre il 90% dei dati europei risiede nelle infrastrutture cloud di aziende statunitensi come Microsoft, Amazon e Google che non sono semplicemente fornitori di servizi, ma sono diventati pilastri dell'infrastruttura digitale europea, fornendo servizi critici che vanno ben oltre il semplice storage di dati.

La questione si complica ulteriormente considerando la crescente complessità tecnologica del panorama digitale. La maggior parte delle organizzazioni europee, sia pubbliche che private, si trova a confrontarsi con una realtà in cui le competenze necessarie per gestire autonomamente la propria sicurezza informatica superano le loro capacità interne.

Rimangono appannaggio di USA, ed in parte Cina, la padronanza delle tecnologie chiave del futuro – dal quantum computing all'intelligenza artificiale, dalla blockchain ai semiconduttori.

L'Europa ha investito significativamente nello sviluppo di infrastrutture cloud sovrane, con il progetto Gaia-X come esempio emblematico. Tuttavia, questa iniziativa sta mostrando significative criticità e rischia di naufragare nonostante le ambizioni iniziali. Questo insuccesso evidenzia la complessità delle sfide e solleva interrogativi sulla reale capacità di sviluppare una vera innovazione alternativa.

Sempre più Stati utilizzano a vari scopi dispositivi IMSI catcher (sistemi di **intercettazione e sorveglianza** finalizzati alla localizzazione dell'utenza telefonica e quindi alla individuazione fisica del titolare), ciò riporta a galla la divisiva e apparentemente irrisolvibile contraddizione tra sicurezza nazionale e diritto alla privacy. Ed anche questi sono sistemi con tecnologie USA.

La crescente sofisticazione dei deepfake creati con l'intelligenza artificiale solleva questioni giuridiche critiche e dibattiti accesissimi riguardanti la privacy e l'identità. Ribadendo il "liberi tutti" statunitense, l'AI Act, sia europeo che italiano, ha normato tutto, tranne l'unico modo per renderci consapevoli, ovvero quello di inserire obbligatoriamente **un bollino di riconoscimento** per le creazioni fatte con l'IA. Il cervello umano le riterrebbe immediatamente informazioni quanto meno da approfondire.

# Conclusioni

Con questi presupposti far vivere la società digitale nel rispetto dello Stato di diritto potrà avvenire se e solo se da un lato riusciremo a vedere sin dall'inizio un sistema con i dati, liberati dalla burocrazia inutile e dannosa, che eliminino le barriere relative alle condizioni di vita sociale, economiche, professionali in cui segmenti della cittadinanza vivono, garantendo la possibilità di migliorare il modo di esserci in modo dinamico (**evolutivo o involutivo)**. In sintesi, politiche per la società digitale che non la pensino come un oggetto tecnocratico.
In conclusione, c'è ancora da riflettere, molto da fare, moltissimo da attuare.

**Bibliografia**


- EU Cybersecurity Strategy for the Digital Decade, 2020
- Digital Services Act, European Commission
- Cyber Resilience Act, European Commission
- European Chips Act, 2023
- NIS2 Directive, European Union
- ENISA Threat Landscape Reports
- ITU Global Cybersecurity Index

N. 3 - 2025 - pp. 83-87

# La dichiarazione sui diritti e i principi digitali per il decennio digitale: una costituzione digitale per l'Europa. Opportunità e rischi di un'interpretazione solamente formale.

**Daniele Napoleone**

**Abstract:** La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, adottata nel 2023, rappresenta un atto politico che delinea una visione comune per guidare la trasformazione digitale dell'Europa nel rispetto dei diritti fondamentali e dei valori democratici. Pur non essendo vincolante, essa si configura come una "costituzione digitale" capace di orientare le politiche nazionali. Tuttavia, il rischio di una ricezione meramente formale è concreto, soprattutto in Paesi come l'Italia, dove spesso le misure sono state adottate in ottica di adempimento burocratico. L'articolo propone di interpretare la Dichiarazione non come un elenco di principi astratti, ma come un quadro operativo da tradurre in politiche concrete, fondate su sostenibilità economica e organizzativa, cooperazione territoriale, valorizzazione delle competenze e strumenti di valutazione dell'impatto. Solo in questo modo essa può diventare una bussola per un digitale europeo realmente a misura di cittadino.

The European Declaration on Digital Rights and Principles for the Digital Decade, adopted in 2023, is a political act outlining a common vision to steer Europe's digital transformation while safeguarding fundamental rights and democratic values. Although not legally binding, it stands as a "digital constitution" to guide national strategies. However, the risk of a merely formal reception is tangible, especially in countries like Italy, where measures are often implemented as bureaucratic compliance. This article argues that the Declaration should not be reduced to a set of abstract statements but rather serve as an operational framework to be translated into concrete policies, grounded in economic and organizational sustainability, territorial cooperation, skill development, and impact evaluation tools. Only in this way can it truly become a compass for a European digital transition tailored to citizens' needs.

**Parole chiave:** diritti digitali, principi digitali, decennio digitale, sostenibilità, governance, inclusione, trasformazione digitale, interoperabilità, valutazione d'impatto, cooperazione territoriale, competenze digitali, partecipazione, trasparenza, sicurezza, intelligenza artificiale.

**Sommario:** 1. Introduzione e principi fondanti; 2. Rischi di formalismo e sfide dell'attuazione; 3. Sostenibilità e governance; 4. Partecipazione e prospettive future

# 1. Introduzione e principi fondanti

Nel gennaio 2023, l'Unione Europea ha adottato la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale. Non si tratta di una norma vincolante in senso stretto, ma di un atto politico che ambisce a tracciare una visione comune, condivisa dagli Stati membri, per orientare la trasformazione digitale del continente nel rispetto dei diritti fondamentali, della dignità umana e dei valori democratici. In altre parole, potremmo definirla una sorta di "costituzione digitale" europea, capace di indicare la rotta in un'epoca di profonda e rapida evoluzione tecnologica.

I principi sanciti nella Dichiarazione toccano temi fondamentali: la centralità della persona, l'inclusione e l'accessibilità, la libertà di scelta, la partecipazione democratica, la sostenibilità ambientale e sociale del digitale, la sicurezza e la protezione nello spazio virtuale. Si tratta di enunciati largamente condivisibili, che delineano un quadro di riferimento etico e politico imprescindibile per una digitalizzazione che non sia solo efficiente, ma anche giusta.

# 2. Rischi di formalismo e sfide dell'attuazione

L'elemento davvero innovativo è che tutti gli Stati membri si siano impegnati a rispettare questi principi, riconoscendoli come valori guida per le rispettive strategie digitali. Tuttavia, proprio in questa adesione formale si annida un possibile rischio: quello di una ricezione superficiale, puramente burocratica, che riduca i principi a liste da spuntare per adempiere a obblighi percepiti come imposti "dall'alto".

In Italia, purtroppo, non sono mancate esperienze di questo tipo in passato. Abbiamo visto troppo spesso misure adottate "perché ce lo chiede l'Europa", svuotate però del significato profondo delle politiche che le ispiravano. Il rischio è che anche la Dichiarazione venga interpretata come un esercizio formale, perdendo il suo potenziale trasformativo.

Questo rischio è ancora più evidente nel contesto attuale, segnato dall'avanzamento accelerato delle tecnologie. Proprio mentre la Commissione Europea vara l'AI Act e altri atti legislativi cruciali, l'affermazione dei diritti digitali come bussola politica assume un'importanza strategica, ma richiede coerenza e profondità nell'attuazione.

# 3. Sostenibilità e governance

Nel caso italiano, l'effettività dell'applicazione di questi principi passa inevitabilmente attraverso la gestione dei fondi pubblici. Le politiche di sviluppo digitale sono spesso legate al Quadro finanziario pluriennale, al PNRR e ai Programmi nazionali cofinanziati dai fondi europei. Questo rende evidente che il tema della **sostenibilità** – non solo ambientale, ma economica e organizzativa – è centrale.

Un esempio concreto dell'importanza dei principi espressi nella Dichiarazione, e in particolare del tema della sostenibilità, emerge chiaramente se si osserva la gestione della spesa del PNRR per la digitalizzazione degli enti locali. In molti casi, i bandi e le misure adottate hanno privilegiato la rapidità di erogazione e l'uniformità di accesso, senza però promuovere in modo incisivo una riflessione strutturale sul modello organizzativo degli enti. Una strategia più lungimirante avrebbe potuto introdurre, ad esempio, meccanismi di premialità per quelle amministrazioni che avessero presentato progetti di semplificazione e riorganizzazione dei servizi, o proposte di accorpamento funzionale a livello territoriale. Interventi di questo tipo non solo avrebbero favorito una maggiore efficienza, ma avrebbero anche aumentato la sostenibilità nel tempo dei risultati ottenuti: una volta esaurito il finanziamento straordinario, infatti, saranno le risorse ordinarie degli enti a dover garantire il funzionamento e l'evoluzione dei sistemi digitali introdotti. Questo esempio mostra come i principi della Dichiarazione non siano solo ideali di riferimento, ma possano e debbano tradursi in criteri operativi per una progettazione pubblica più coerente, solida e duratura.

Questi ragionamenti assumono ancora maggiore rilevanza se si considera l'eterogeneità del nostro territorio e delle sue amministrazioni. Il rischio di una transizione digitale "a taglia unica", indifferente alle differenze strutturali tra grandi centri urbani e piccoli comuni, è più che concreto. Non tutti gli enti locali partono dallo stesso livello di maturità digitale, né dispongono delle medesime risorse organizzative. In questo contesto, i principi di inclusione, equità e sostenibilità evocati dalla Dichiarazione europea dovrebbero tradursi in **politiche pubbliche differenziate e mirate**, capaci di sostenere chi è strutturalmente più fragile, ad esempio incentivando la cooperazione tra enti o forme di gestione associata dei servizi digitali. Anche questo sarebbe un modo per rendere effettivi i diritti digitali e non solo proclamarli.

Per questo, una strategia realmente sostenibile dovrebbe incentivare, sin dalla fase di progettazione, interventi mirati alla semplificazione, alla cooperazione intercomunale e alla razionalizzazione delle funzioni. La capacità di innovare, in fondo, non è solo tecnologica, ma anche, o forse soprattutto, istituzionale e relazionale. Ed è responsabilità della politica definire criteri e strumenti che promuovano questi aspetti, traducendoli in requisiti premianti nelle misure come quelle del PNRR. Solo così si può passare da una logica di spesa a una vera logica di investimento, dove le risorse pubbliche non si limitano a finanziare progetti temporanei, ma costruiscono

valore e capacità durature per il sistema pubblico.

Accanto a ciò, un altro elemento spesso trascurato riguarda la **cultura della valutazione**. Troppo spesso la digitalizzazione viene misurata in termini di quantità di fondi spesi o numero di servizi attivati, senza una reale attenzione agli impatti generati. Una piena adesione allo spirito della Dichiarazione richiederebbe invece che ogni intervento fosse accompagnato da strumenti di **valutazione ex ante ed ex post**, che misurino non solo l'efficienza economica, ma anche la qualità dell'accesso, l'effettivo esercizio dei diritti digitali, la trasparenza e l'usabilità dei servizi. Non si tratta solo di rispettare parametri formali, ma di garantire che gli interventi pubblici abbiano una ricaduta positiva e misurabile sulla vita dei cittadini.

Nessuna transizione digitale, inoltre, sarà davvero sostenibile se non si investe anche nella formazione del personale delle amministrazioni, nella capacità di attrarre e trattenere figure tecniche qualificate e nella creazione di team multidisciplinari che sappiano tradurre le esigenze amministrative in soluzioni tecnologiche coerenti con i diritti digitali. Il tema delle **competenze e del capitale umano** vale a maggior ragione per i piccoli enti, che spesso si trovano a gestire progetti complessi senza il supporto adeguato.

# 4. Partecipazione e prospettive future

Un elemento trasversale a tutti i precedenti è quello della **partecipazione e della cittadinanza attiva**. La Dichiarazione richiama esplicitamente l'importanza di rafforzare la democrazia digitale, promuovere la trasparenza e combattere la disinformazione. Ma perché ciò accada, è necessario che anche i cittadini siano messi nelle condizioni di comprendere, controllare e contribuire allo sviluppo dei servizi digitali. La digitalizzazione pubblica non deve essere solo un processo tecnico, ma anche un'occasione per **ripensare il rapporto tra istituzioni e cittadini**, favorendo processi partecipativi e forme nuove di accountability.

Tutti questi aspetti non possono essere delegati alla sola normativa europea o affidati passivamente al corso delle tecnologie. È responsabilità della politica nazionale, nel definire strategie e allocazioni di risorse – come nel caso del PNRR – assicurarsi che **i criteri di sostenibilità, cooperazione territoriale, valutazione e competenze siano parte integrante dei processi decisionali**, affinché si possa passare da una logica di spesa a una logica di vero investimento per il futuro.

Se si parte da questi presupposti, allora la Dichiarazione sui diritti digitali – insieme agli altri atti europei come il Data Governance Act, l'AI Act o il Digital Services Act – non rappresentano solo riferimenti astratti, ma possono diventare **griglie va-**

**loriali e funzionali** per guidare lo sviluppo di soluzioni digitali realmente coerenti con la visione europea. Una visione in cui l'innovazione non si contrappone ai diritti, ma li rafforza. Una visione che richiede più progettualità e meno adempimenti, più coerenza e meno formalismi.

La sfida è aperta: sta ai decisori pubblici, ai giuristi, ai progettisti digitali e alla società civile interpretare questi principi non come vincoli, ma come **opportunità per costruire un digitale europeo davvero a misura di cittadino e tramutare una visione in un percorso di sviluppo strategico**.

N. 3 - 2025 - pp. 88-111

# Il paradigma europeo della sicurezza digitale tra *security by design* e autodeterminazione informazionale: riflessioni critiche sul Capitolo V della Dichiarazione europea sui diritti e principi digitali

**Enrica Priolo**

**Abstract:** La Dichiarazione europea sui diritti e principi digitali per il decennio digitale configura un modello di governance tecnologica che tenta di conciliare le esigenze di sicurezza sistemica con l'autodeterminazione individuale. Il presente contributo analizza criticamente il paradigma "sicurezza-protezione-responsabilizzazione" delineato nel Capitolo V, evidenziandone le implicazioni giuridico-economiche e le tensioni dialettiche tra tutela eteronoma e autonomia soggettiva nell'ecosistema digitale europeo, con particolare attenzione alle criticità emergenti dal binomio empowerment/marketing digitale.

The european Declaration on digital rights and principles for the digital decade configures a technological governance framework that seeks to reconcile systemic security imperatives with individual self-determination. The present contribution critically examines the "security-protection-empowerment" paradigm delineated in Chapter V, elucidating its juridical-economic implications and the dialectical tensions between heteronomous safeguarding and subjective autonomy within the European digital ecosystem, with particular emphasis on the emergent criticalities stemming from the empowerment/digital marketing dyad.

## 1. Premessa metodologica

La Dichiarazione europea sui diritti e principi digitali per il decennio digitale, proclamata congiuntamente da Parlamento, Consiglio e Commissione europea il 23 gennaio 2023[1], rappresenta un *unicum* nel panorama della regolazione sovranazio-

[1] Dichiarazione europea sui diritti e principi digitali per il decennio digitale (2023/C 23/01), in

nale del digitale. Si tratta, più che di un documento programmatico, di un vero e proprio *constitutional moment*[2] che cristallizza l'approccio valoriale europeo alla *governance* tecnologica in un contesto di crescente frammentazione normativa globale[3].

Il documento si inserisce nel solco della tradizione costituzionale europea che, sin dal Trattato di Lisbona, ha fatto della tutela dei diritti fondamentali nell'era digitale uno dei pilastri dell'integrazione sovranazionale. Tuttavia, la Dichiarazione presenta caratteri di novità significativi rispetto alla precedente produzione normativa europea, configurandosi come il primo tentativo organico di elaborazione di un *bill of rights* digitale che trascenda la dimensione meramente regolativa per abbracciare una visione costituzionale del rapporto tra tecnologia e diritti umani[4].

Il Capitolo V, dedicato alla "Sicurezza, protezione e responsabilizzazione" (*Safety, security and empowerment*), costituisce il nucleo teoretico più denso dell'intero impianto normativo, configurando un paradigma di tutela che trascende la tradizionale dicotomia pubblico-privato per abbracciare una visione sistemica della sicurezza digitale come *public good*. La scelta di utilizzare il termine inglese *empowerment* - non tradotto nelle versioni linguistiche nazionali - segnala l'adozione di un concetto giuridico autonomo che non trova corrispondenza nella tradizione continentale europea[5].

La scelta lessicale non è neutra: l'uso del termine *empowerment* - mutuato dalla tradizione anglosassone delle *capabilities theories*[6]- segnala l'adozione di un approccio che privilegia la dimensione sostanziale dell'autonomia soggettiva rispetto alla mera libertà formale di scelta. Questa opzione metodologica comporta significative implicazioni per l'interpretazione sistematica dell'intero documento, orientando l'ermeneutica giuridica verso una concezione *outcome-based* piuttosto che *process-based* dei diritti digitali[7].

Tuttavia, l'adozione acritica del concetto di *empowerment* pone questioni circa

Gazzetta Ufficiale dell'Unione europea, C 23/1, 23 gennaio 2023.

[2] Sul concetto di *constitutional moment* nell'evoluzione del diritto europeo cfr. N. WALKER, Constitutional Pluralism, in Journal of Constitutional Theory, 2002, p. 317 ss.

[3] Sulla frammentazione della governance digitale globale cfr. A. BRADFORD, The Brussels effect: how the European Union rules the world, Oxford University Press, 2020.

[4] Cfr. O. POLLICINO, Constitutional Law in the Age of Balancing, in European Law Journal, 2010, p. 16 ss.

[5] Sulla traduzione giuridica dei concetti di empowerment cfr. M. NUSSBAUM, Creating capabilities: the human development approach, Harvard University Press, 2011.

[6] A. SEN, Development as freedom, Oxford University Press, 1999; M. NUSSBAUM, Women and human development, Cambridge University Press, 2000.

[7] Sulla distinzione tra approcci outcome-based e process-based cfr. J. RAWLS, A Theory of Justice, Harvard University Press, 1970.

la sua traduzione operativa nell'ordinamento giuridico europeo. La dottrina costituzionalistica ha da tempo evidenziato le difficoltà di conciliare l'approccio *capabilities-based* con i principi dello Stato di diritto liberale, particolarmente per quanto attiene alla definizione dei parametri oggettivi di valutazione dell'*empowerment* effettivo[8].

# 2. Come la sicurezza digitale passa dalla *privacy by design* alla *dignity by design*

## 2.1 Il paradigma della sicurezza sistemica e la rivoluzione del *by design*

L'articolo 16 della Dichiarazione postula un diritto di accesso a "tecnologie, prodotti e servizi digitali che siano sicuri, protetti e rispettosi della privacy fin dalla progettazione". Questa formulazione configura una vera e propria rivoluzione copernicana nella concezione della sicurezza digitale che da attributo contingente e *ex post* diventa requisito strutturale e *ex ante*.

Il principio della *security by design* si radica nella tradizione costituzionale europea della protezione proattiva dei diritti fondamentali, già cristallizzata nell'art. 25 del GDPR. La *data protection by design and by default* rappresenta, infatti, il precedente normativo più significativo di questo approccio, configurando un obbligo per i titolari del trattamento di integrare le garanzie di protezione dati sin dalla fase progettuale dei sistemi informatici[9].

Però la Dichiarazione amplia significativamente il perimetro applicativo, estendendo l'obbligo di sicurezza progettuale dall'ambito specifico della protezione dati all'intero ecosistema digitale. Questa estensione comporta implicazioni giuridiche di grande portata, configurando un nuovo esempio di responsabilità che si estende a tutti gli attori della filiera tecnologica: dai produttori di hardware ai fornitori di software, dai gestori di piattaforme agli intermediari della rete[10].

Dal punto di vista dell'analisi economica del diritto, questa scelta comporta una

---

[8] Cfr. S. HOLMES, C. SUNSTEIN, The Cost of Rights: Why Liberty Depends on Taxes, W.W. Norton, 1999.

[9] Cfr. A. CAVOUKIAN, Privacy by Design: The 7 Foundational Principles, Information and Privacy Commissioner of Ontario, 2009.

[10] Sulla responsabilità nella filiera tecnologica cfr. F. PASQUALE, The Black Box Society, Harvard University Press, 2015.

significativa alterazione degli incentivi di mercato: la sicurezza digitale da esternalità negativa - tradizionalmente scaricata sui consumatori finali[11]- diventa costo di produzione internalizzato *ex lege*. Si configura, così, un modello di *full cost accounting* che riflette il vero costo sociale delle tecnologie digitali, correggendo le distorsioni allocative generate dal tradizionale modello di *negative externalities shifting*[12].

La letteratura economica ha ampiamente dimostrato come l'internalizzazione delle esternalità negative attraverso meccanismi normativi possa generare effetti di efficienza allocativa superiori rispetto ai meccanismi di mercato puro[13]. Nel caso specifico della sicurezza digitale, l'obbligo di *security by design* configura una forma di *Pigouvian regulation* che corregge il fallimento del mercato nella produzione di sicurezza informatica[14].

Epperò l'implementazione pratica di questo paradigma presenta difficoltà significative, particolarmente per quanto attiene alla definizione degli standard tecnici di sicurezza. La Dichiarazione non fornisce indicazioni specifiche circa i parametri di valutazione della sicurezza *by design*, demandando presumibilmente alla normativa di attuazione la specificazione tecnica dei requisiti.

## 2.2 Il problema del *regulatory lag*

Inoltre, l'implementazione del paradigma *by design* ci fa interrogare sul rapporto tra standardizzazione normativa e dinamismo innovativo. La letteratura economica ha da tempo evidenziato il trade-off tra *regulatory certainty* e *innovation incentives* nei mercati tecnologici caratterizzati da rapida obsolescenza[15].

Il fenomeno del *regulatory lag* - il ritardo strutturale della regolazione rispetto all'evoluzione tecnologica - assume particolare rilevanza nell'ambito della sicurezza digitale, in cui l'efficacia delle misure protettive dipende criticamente dall'aggiornamento continuo rispetto alle minacce emergenti[16]. La rigidità degli strumenti normativi tradizionali mal si concilia con la velocità di evoluzione delle tecnologie digitali e delle relative vulnerabilità.

---

[11] Sul fenomeno delle esternalità negative in ambito digitale cfr. T. WU, The Attention Merchants, Vintage Books, 2016

[12] Cfr. A. PIGOU, *The economics of welfare*, Macmillan, 1920.

[13] R. COASE, *The problem of social cost*, in *Journal of Law and Economics*, 1960, p. 1 ss.

[14] Sul concetto di *Pigouvian regulation* cfr. W. BAUMOL, W. OATES, *The Theory of Environmental Policy*, Cambridge University Press, 1988.

[15] Cfr. P. AGHION, N. BLOOM, R. BLUNDELL, R. GRIFFITH, P. HOWITT, *Competition and innovation: an inverted-U relationship*, in *The quarterly journal of economics*, 2005, p. 701 ss.

[16] Sul *regulatory lag* nel settore digitale cfr. L. LESSIG, *Code: version 2.0*, Basic Books, 2006.

La Dichiarazione tenta di risolvere questa tensione attraverso il ricorso al concetto di "requisiti appropriati di sicurezza informatica per i prodotti connessi immessi sul mercato unico" (art. 16, lett. b), che configura un sistema di regolazione adattiva basato su standard tecnici evolutivi anzichè su prescrizioni normative rigide.

Questo approccio si allinea con la tradizione europea del "nuovo approccio" alla standardizzazione tecnica, inaugurato dalla Risoluzione del Consiglio del 7 maggio 1985 che privilegia la definizione di requisiti essenziali di sicurezza lasciando agli organismi di standardizzazione la specificazione tecnica dei mezzi per raggiungerli. Il modello del *New Legislative Framework* europeo, consolidato dal Regolamento (CE) n. 765/2008, fornisce il quadro procedurale per l'elaborazione di standard tecnici armonizzati che garantiscano la presunzione di conformità ai requisiti essenziali.

Ma l'applicazione di questo modello al settore digitale presenta specificità che ne complicano l'implementazione. A differenza dei settori tradizionali – in cui la standardizzazione tecnica si concentra su prodotti fisici con caratteristiche relativamente stabili - il settore digitale è caratterizzato da prodotti immateriali (software, algoritmi, protocolli) soggetti a continua evoluzione[17].

La natura *layered* dell'architettura digitale - che comprende livelli hardware, software, protocolli di rete, applicazioni e interfacce utente - richiede un approccio sistemico alla standardizzazione che tenga conto delle interdipendenze tra i diversi strati tecnologici. Questa complessità sistemica genera rischi di *standard conflicts* e *interoperability failures* che possono compromettere l'efficacia complessiva delle misure di sicurezza[18].

## 2.3 Il nesso tra sicurezza e marketing digitale: dalle vulnerabilità tecniche alle vulnerabilità cognitive

Un aspetto particolarmente critico del paradigma della sicurezza *by design* emerge dal suo rapporto con le strategie di marketing digitale. La Dichiarazione, pur non affrontando esplicitamente questa problematica, contiene riferimenti che evidenziano la tensione tra le esigenze di sicurezza dell'utente e le logiche di mercato che governano l'economia digitale.

---

[17] Sulla specificità della standardizzazione digitale cfr. C. SHAPIRO, H. VARIAN, *Information rules*, Harvard Business School Press, 1999.

[18] Sul problema dell'interoperabilità cfr. J. PALFREY, U. GASSER, *Interop: the promise and perils of highly interconnected Systems*, Basic Books, 2012.

L'articolo 15, lett. f) fa riferimento alla necessità di "limitare lo sfruttamento delle vulnerabilità e dei pregiudizi, in particolare attraverso la pubblicità mirata". Questa disposizione configura un'estensione del concetto di sicurezza digitale dalle vulnerabilità tecniche a quelle cognitive, aprendo questioni inedite circa i limiti della manipolazione commerciale nell'ecosistema digitale[19].

La letteratura di economia comportamentale ha ampiamente documentato come le tecniche di *behavioral targeting* utilizzate nel marketing digitale sfruttino sistematicamente le *cognitive biases* degli utenti per orientarne le scelte di consumo[20]. Tecniche come il *loss aversion framing*, il *social proof manipulation*, l'*anchoring effect* e il *scarcity principle* rappresentano forme di manipolazione psicologica che compromettono l'autonomia decisionale degli individui[21].

Il riconoscimento di queste vulnerabilità cognitive come oggetto di tutela giuridica configura una significativa evoluzione del concetto di sicurezza digitale che trascende la dimensione tecnico-informatica per abbracciare la protezione dell'integrità psicologica dell'utente[22]. Tuttavia, questa estensione pone interrogativi circa i criteri di identificazione delle pratiche manipolative e i limiti della libertà commerciale nell'ambiente digitale[23].

# 3. La privacy come diritto di controllo

## 3.1 Dalla *informational self-determination* alla *digital sovereignty*

L'articolo 17 della Dichiarazione configura la privacy non meramente come diritto all'esclusione, ma come "controllo da parte degli individui su come i loro dati personali vengono utilizzati e con chi vengono condivisi". Questa formulazione segna un'evoluzione significativa rispetto alla tradizionale concezione proprietaria del dato, abbracciando una visione relazionale della privacy come *jus excludendi alios*

---

[19] Sulla manipolazione cognitiva nel marketing digitale cfr. S. ZUBOFF, *The age of surveillance capitalism*, PublicAffairs, 2019.

[20] Cfr. R. THALER, C. SUNSTEIN, *Nudge: improving decisions about health, wealth, and happiness*, Yale University Press, 2008.

[21] D. KAHNEMAN, *Thinking, Fast and Slow*, Farrar, Straus and Giroux, 2011.

[22] Sulla protezione dell'integrità psicologica cfr. J. COHEN, *Semantic Discontinuity in the Law of Privacy*, in *University of Chicago Law Review*, 2010, p. 77 ss.

[23] Sui limiti della libertà commerciale nell'ambiente digitale cfr. N. HELBERGER, *On the democratic role of news recommenders*, in *Digital Journalism*, 2019, p. 993 ss.

dinamico e contestuale.

La nozione di controllo (*control*) utilizzata dalla Dichiarazione si radica nella dottrina tedesca dell'*informationelle Selbstbestimmung* elaborata dal Bundesverfassungsgericht nella decisiva sentenza del 1983 sul censimento federale. Secondo questa concezione, il diritto alla protezione dati non si esaurisce nella dimensione defensiva, ma comprende una componente positiva che conferisce all'individuo la facoltà di determinare le modalità di utilizzo delle informazioni che lo riguardano.

La dottrina costituzionalistica europea, poi, ha già riconosciuto nella protezione dei dati personali una nuova categoria di diritti fondamentali, distinta sia dai diritti di libertà che dai diritti sociali[24]. La sentenza della Corte di Giustizia UE nei casi congiunti Google Spain (C-131/12) e Schrems I (C-362/14) ha chiarito che la protezione dati non può essere ridotta a mero bilanciamento con altri interessi, ma costituisce un valore autonomo dell'ordinamento europeo che gode di una *presunzione di prevalenza* negli eventuali conflitti con interessi economici.

Ebbene, la Dichiarazione radicalizza questa prospettiva, configurando il controllo sui dati come presupposto necessario per l'esercizio dell'autodeterminazione informazionale. Si delinea, quindi, una concezione della privacy come *empowerment right* che trascende la dimensione difensiva per assumere carattere costitutivo dell'identità digitale[25].

Tuttavia, la traduzione operativa di questo paradigma presenta diverse complessità, soprattutto in relazione ai modelli di business basati sulla monetizzazione dei dati personali. Il paradigma del controllo presuppone infatti una capacità di scelta informata e consapevole che entra in tensione con la complessità tecnica dei sistemi di trattamento dati e l'asimmetria informativa strutturale tra utenti e piattaforme[26].

## 3.2 Sul consenso informato nell'economia dell'attenzione

La centralità del controllo individuale sui dati personali pone in evidenza le criticità del meccanismo del consenso informato come strumento di tutela della privacy. La ricerca empirica ha ampiamente documentato i limiti cognitivi del consenso nell'ambiente digitale, evidenziando come la maggior parte degli utenti non legga le

[24] Cfr. G. GONZÁLEZ FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014.

[25] Sulla privacy come *empowerment right* cfr. J. COHEN, *What Privacy is For*, in *Harvard Law Review*, 2013.

[26] Sull'asimmetria informativa nel settore digitale cfr. A. ACQUISTI, L. BRANDIMARTE, G. LOEWENSTEIN, *Privacy and human behavior in the age of information*, in *Science*, 2015.

informative privacy e acconsenta ai trattamenti senza una reale comprensione delle implicazioni[27].

Il fenomeno della *privacy paradox* - la discrepanza tra le preferenze di privacy dichiarate e i comportamenti effettivi degli utenti[28] - evidenzia l'inadeguatezza del modello del consenso informato come strumento di *empowerment* nell'ecosistema digitale. Dal canto suo, la *behavioral economics* ha dimostrato come fattori quali la *present bias*, l'*hyperbolic discounting* e la *cognitive overload* compromettano sistematicamente la capacità degli individui di effettuare scelte razionali in materia di privacy[29].

Questa problematica assume particolare rilevanza nel contesto del marketing digitale, dove le tecniche di *dark patterns* sono specificamente progettate per manipolare il processo decisionale degli utenti e ottenere consensi che non riflettono le loro reali preferenze. Pratiche come il *pre-checked boxes*, il *roach motel design*, il *bait and switch* e il *forced continuity* rappresentano forme di manipolazione dell'architettura della scelta che compromettono l'autenticità del consenso.

La dottrina giuridica ha iniziato a elaborare criteri per la valutazione della validità del consenso che tengano conto di queste distorsioni cognitive. Il principio del *genuine choice*, elaborato dalla giurisprudenza della Corte di Giustizia UE[30], richiede che il consenso sia espresso in condizioni che garantiscano l'effettiva libertà di scelta, escludendo situazioni di dipendenza economica o psicologica che ne compromettano l'autenticità[31].

## 3.3 Il diritto alla successione digitale: verso l'immortalità controllata

Di particolare originalità teoretica è il riconoscimento del diritto alla determinazione della "eredità digitale" (*digital legacy*) di cui all'articolo 19. Questa disposizione configura una proiezione della sovranità digitale oltre i confini temporali

---

[27] Cfr. L. MCDONALD, Y. CRANOR, *The cost of reading privacy policies*, in *I/S: A Journal of Law and Policy for the Information Society*, 2008.

[28] S. KOKOLAKIS, *Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon*, in *Computers & Security*, 2017, p. 122 ss.

[29] Cfr. A. ACQUISTI, L. BRANDIMARTE, G. LOEWENSTEIN, *Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age*, in *Journal of Consumer Psychology*, 2020, p. 736 ss.

[30] Corte di Giustizia UE, sentenza 1° ottobre 2019, causa C-673/17, *Planet49*.

[31] Cfr. N. HELBERGER, F. ZUIDERVEEN BORGESIUS, A. REYNA, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, in *Common Market Law Review*, 2017, p. 1427 ss.

dell'esistenza biologica, ponendo questioni inedite circa la natura giuridica dell'identità post-mortem nell'era digitale[32].

Il diritto successorio tradizionale si è strutturato attorno alla distinzione tra *res corporales* e *res incorporales*, categoria quest'ultima che include i diritti patrimoniali ma esclude tradizionalmente i diritti della personalità per la loro natura strettamente personale[33]. L'identità digitale sfugge a questa tassonomia, configurandosi come *tertium genus* che partecipa simultaneamente della dimensione patrimoniale (valore economico dei profili social, degli account, del *digital estate*) e di quella personalissima (espressione dell'identità, della reputazione, della memoria individuale)[34].

La soluzione prospettata dalla Dichiarazione - la determinazione soggettiva del destino post-mortem dell'identità digitale - configura una sorta di "testamento digitale" che estende l'autonomia privata al governo della propria persistenza informazionale[35]. Si tratta di un'innovazione di portata rivoluzionaria che anticipa sviluppi normativi destinati ad assumere crescente rilevanza con l'espansione dell'Internet of Things e dell'intelligenza artificiale[36].

Tuttavia, l'implementazione pratica di questo diritto presenta complessità significative, particolarmente in relazione agli aspetti transnazionali della successione digitale. La maggior parte dei servizi digitali è fornita da società con sede in giurisdizioni extraeuropee, che applicano normative successorie diverse da quelle europee[37]. La frammentazione normativa internazionale in materia di successione digitale genera rischi di *forum shopping* e conflitti di legge che possono compromettere l'effettività del diritto riconosciuto dalla Dichiarazione.

## 3.4 La profilazione post-mortem e le nuove frontiere dell'exploitation commerciale

Un aspetto particolarmente critico del diritto alla successione digitale emerge dal suo rapporto con le strategie di marketing digitale basate sulla profilazione degli

---

[32] Sulla successione digitale cfr. J. CARROLL, R. ROMANO, *Your Digital Afterlife*, New Riders, 2011.

[33] Cfr. A. TORRENTE, P. SCHLESINGER, *Manuale di diritto privato*, Giuffrè, 2019.

[34] Sul concetto di *digital estate* cfr. E. HARBINJA, *Legal aspects of transmission of digital assets on death*, University of Strathclyde, 2017.

[35] Cfr. D. LAMETTI, *The Concept of Property: Relations Through Objects of Social Wealth*, in *University of Toronto Law Journal*, 2003, p. 325 ss.

[36] Cfr. R. WALKER, *The Rights and Duties of Electronic Personality*, in *John Marshall Journal of Computer & Information Law*, 2014, p. 397 ss.

[37] Sulla frammentazione normativa internazionale cfr. P. SWIRE, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, in *International Lawyer*, 1998, p. 991 ss.

utenti deceduti. La ricerca ha evidenziato come le piattaforme digitali continuino a raccogliere e processare dati relativi agli utenti deceduti attraverso l'analisi dei comportamenti dei loro contatti sociali, configurando forme di profilazione per prossimità che estendono il targeting commerciale oltre la morte[38].

Questa pratica solleva problematiche circa i limiti temporali della protezione dati e la legittimità dello sfruttamento commerciale dell'identità digitale post-mortem. Il diritto alla determinazione della *digital legacy* riconosciuto dalla Dichiarazione potrebbe configurare uno strumento di tutela contro queste forme di exploitation commerciale, estendendo la sovranità digitale del soggetto oltre i confini dell'esistenza biologica[39].

# 4. L'empowerment come categoria giuridica

## 4.1 La dimensione costitutiva dell'empowerment digitale e le sue radici teoriche

Il concetto di *empowerment* che permea l'intero Capitolo V non può essere ridotto ad una traduzione della nozione sociologica di *empowerment*, ma assume una specifica valenza giuridico-costituzionale nell'ordinamento europeo[40]. L'*empowerment* digitale si configura come una nuova categoria di diritti che presuppone non solo la titolarità formale di prerogative soggettive, ma la capacità sostanziale di esercitarle attraverso competenze, strumenti e condizioni ambientali adeguati.

Questa concezione si radica nella tradizione del *social constitutionalism* europeo che ha da tempo superato la distinzione liberale classica tra libertà negative e positive per abbracciare una visione integrata dei diritti fondamentali come presupposti per l'autorealizzazione personale[41]. L'art. 3, comma 2, della Costituzione italiana, che impone alla Repubblica di "rimuovere gli ostacoli di ordine economico e sociale" che impediscono il pieno sviluppo della persona umana, costituisce il prototipo normativo di questa concezione sostanziale della libertà.

---

[38] Sulla profilazione post-mortem cfr. D. CARROLL, J. MOORE, The apps of the dead: a study on mobile app privacy policies and the handling of digital remains, in Death Studies, 2015.

[39] Sulla sovranità digitale post-mortem cfr. T. BELL, Life, Death, and Property on the Internet, in Stanford Technology Law Review, 2014.

[40] Sull'empowerment come categoria giuridica cfr. M. MINOW, Making All the Difference: Inclusion, Exclusion, and American Law, Cornell University Press, 1990.

[41] Sul social constitutionalism europeo cfr. C. JOERGES, What is left of the european economic constitution?, in European Law Review, 2005, p. 461 ss.

La Dichiarazione europea trasla questo paradigma nell'ecosistema digitale, configurando l'empowerment come **capacità di fare scelte informate** (art. 9) che presuppone tanto l'accesso alle informazioni quanto le competenze cognitive per processarle criticamente. Questa formulazione evidenzia l'influenza della *capabilities approach* di Amartya Sen e Martha Nussbaum[42] che concepisce la libertà non come assenza di costrizioni esterne, ma come effettiva capacità di perseguire i propri progetti di vita[43].

L'adozione di questo paradigma comporta significative implicazioni per l'interpretazione dei diritti digitali, orientando l'analisi giuridica verso una valutazione *outcome-based* dell'effettività delle tutele piuttosto che verso una mera verifica *process-based* della correttezza formale delle procedure. Ci si chiede come verranno formulati i criteri di valutazione dell'empowerment effettivo e la legittimazione democratica delle autorità chiamate a definire tali criteri[44].

## 4.2 Empowerment e asimmetrie informative

L'effettività dell'empowerment digitale presuppone il possesso di competenze cognitive e tecniche che consentano agli individui di navigare consapevolmente l'ecosistema digitale. La *digital literacy* non si esaurisce nella capacità di utilizzare strumenti tecnologici, ma comprende competenze di *media literacy*, *data literacy* e *algorithmic literacy* che abilitano una comprensione critica dei meccanismi che governano l'ambiente digitale.

La ricerca empirica ha evidenziato significative disparità nella distribuzione di queste competenze che si correlano con variabili demografiche, socioeconomiche e geografiche[45]. Il *digital divide* non è più solo una questione di accesso alle tecnologie, ma sempre più una questione di disparità nelle competenze necessarie per utilizzarle efficacemente.

Questa problematica assume particolare rilevanza nel contesto del marketing digitale in cui l'efficacia delle strategie persuasive dipende inversamente dal livello di *digital literacy* del target. Gli utenti con minori competenze digitali sono più vulnerabili alle tecniche di manipolazione cognitiva e meno capaci di riconoscere e

---

[42] A. SEN, Development as freedom, cit.; M. NUSSBAUM, Creating capabilities, cit.

[43] Cfr. I. ROBEYNS, The Capability Approach: A Theoretical Survey, in Journal of Human Development, 2005, p. 93 ss.

[44] Cfr. S. HOLMES, C. SUNSTEIN, *The Cost of Rights*, cit.

[45] Sul digital divide cfr. P. NORRIS, Digital divide: civic engagement, information poverty, and the internet worldwide, Cambridge University Press, 2001.

contrastare le pratiche di *dark patterns*[46].

La Dichiarazione riconosce questa problematica nell'articolo 4 che sancisce il diritto di "tutti" ad acquisire competenze digitali di base e avanzate. Tuttavia, il documento non specifica le modalità di implementazione di questo diritto né identifica i soggetti responsabili della sua attuazione. Si configura così un *implementation gap* che rischia di svuotare di significato il principio dell'empowerment digitale.

## 4.3 La protezione dell'infanzia digitale funge da laboratorio dell'empowerment e paradigma del marketing responsabile

Il sottoinsieme normativo dedicato alla "Protezione e responsabilizzazione di bambini e giovani nell'ambiente digitale" (artt. 20-22) costituisce il banco di prova più significativo del paradigma dell'empowerment. La disciplina supera la tradizionale concezione paternalistica della protezione minorile per abbracciare una visione che riconosce nei minori soggetti attivi di diritti digitali[47].

L'articolo 20 configura i minori come soggetti "responsabilizzati a fare scelte sicure e informate ed esprimere la propria creatività nell'ambiente digitale". Tale formulazione segna una discontinuità rispetto alla tradizione giuridica continentale che ha sempre privilegiato la protezione eteronoma dei minori rispetto alla loro autonomia decisionale.

La scelta di utilizzare il termine *empowerment* anche in relazione ai minori segnala l'adozione di un approccio *rights-based* mutuato dalla Convenzione sui diritti del fanciullo del 1989, che riconosce nel minore un soggetto titolare di diritti propri e non oggetto di protezione da parte degli adulti. L'art. 12 della Convenzione, che sancisce il diritto del fanciullo ad esprimere liberamente la propria opinione su ogni questione che lo interessa, costituisce il fondamento normativo di questa concezione[87].

Dal punto di vista economico, questa concezione comporta significative implicazioni per le strategie di *digital marketing* rivolte ai minori. L'articolo 22, lett. d) vieta espressamente il "tracciamento, profilazione e targeting illegali, in particolare a fini commerciali" nei confronti dei minori, configurando una zona franca rispetto alle logiche di mercato che governano l'economia digitale degli adulti.

---

[46] Cfr. C. LUGURI, L. STRAHILEVITZ, Shining a light on dark patterns, in Journal of Legal Analysis, 2021.

[47] Sulla concezione rights-based della protezione minorile cfr. M. FREEMAN, The rights and wrongs of children, Frances Pinter, 1983.

Nondimeno, l'implementazione pratica di questo divieto presenta difficoltà rilevanti, particolarmente in relazione alla verifica dell'età degli utenti online[48]. La maggior parte delle piattaforme digitali utilizza sistemi di *age verification* basati sull'autodichiarazione, facilmente aggirabili dai minori. L'introduzione di sistemi più affidabili di verifica dell'età comporterebbe costi significativi e porrebbe questioni di privacy per tutti gli utenti.

## 4.4 Il "kids marketing" nell'era digitale

Il rapporto tra empowerment dei minori e marketing digitale evidenzia le contraddizioni più acute del modello delineato dalla Dichiarazione. L'industria del marketing digitale ha sviluppato tecniche sempre più sofisticate per influenzare i comportamenti di consumo dei minori, sfruttando la loro maggiore vulnerabilità cognitiva e la loro familiarità con gli strumenti digitali.

Le tecniche di *advergaming*, *influencer marketing*, *native advertising* e *social commerce* rappresentano forme di comunicazione commerciale particolarmente insidiose perché sfumano la distinzione tra contenuto editoriale e messaggio pubblicitario. I minori, per le loro limitate capacità di *media literacy*, sono meno capaci di riconoscere la natura commerciale di questi contenuti e più vulnerabili ai loro effetti persuasivi[49].

La Dichiarazione europea tenta di conciliare la protezione dei minori con il loro empowerment attraverso l'imposizione di obblighi di *age-appropriate design* e la promozione della *media literacy*. Si evidenzia, però, che questo approccio presenta il rischio di scaricare sui minori stessi la responsabilità della propria protezione, configurando una forma di empowerment responsabilizzante che può risultare inadeguata rispetto alla loro effettiva capacità di autodifesa[50].

---

[48] Sull'age verification cfr. A. MORRIS, Age verification for online services, Foundation for Information Policy Research, 2019

[49] Sulla media literacy dei minori cfr. J. POTTER, Media literacy, SAGE Publications, 2016

[50] Sul rischio di "empowerment responsabilizzante" cfr. N. ROSE, Governing the soul, Routledge, 1999

# 5. Le aporie del sistema

## 5.1 I limiti del *libertarian paternalism*

Nonostante l'eleganza teoretica della costruzione, il sistema delineato dalla Dichiarazione presenta alcune aporie strutturali che meritano attenzione critica. La tensione più evidente emerge tra l'aspirazione all'empowerment individuale e la necessità di protezioni eteronome, particolarmente evidente nella disciplina delle "vulnerabilità e pregiudizi" di cui all'art. 15, lett. f).

Il riconoscimento di vulnerabilità cognitive soggettive che giustificano limitazioni all'autonomia decisionale configura una forma di *libertarian paternalism*[51] che, pur trovando giustificazione nella letteratura di economia comportamentale, cozza con i limiti dell'autonomia individuale negli ecosistemi digitali.

La dottrina del *libertarian paternalism*, elaborata da Richard Thaler e Cass Sunstein, sostiene la legittimità di interventi normativi volti a correggere le distorsioni cognitive individuali purché preservino formalmente la libertà di scelta. Secondo questa concezione, è possibile spingere dolcemente (*nudge*) gli individui verso scelte più razionali attraverso la progettazione dell'architettura decisionale, senza limitare le opzioni disponibili.

Ma l'applicazione di questo schema all'ecosistema digitale rischia di configurare una forma di autonomia guidata che svuota di significato il principio stesso dell'autodeterminazione[52]. La natura pervasiva e invisibile degli algoritmi di personalizzazione rende difficile distinguere tra nudge legittimi e manipolazione cognitiva, creando una zona grigia normativa che può essere sfruttata per giustificare forme sottili di controllo comportamentale.

## 5.2 E l'uguaglianza digitale?

Un'ulteriore aporia emerge dal rapporto tra la personalizzazione algoritmica - sempre più pervasiva nell'economia digitale - e il principio di non discriminazione. L'articolo 9, lett. c) impone che "i sistemi algoritmici siano basati su dataset adeguati per evitare la discriminazione", configurando un obbligo di *algorithmic fairness* che

[51] Sul libertarian paternalism cfr. C. SUNSTEIN, R. THALER, Libertarian paternalism is not an oxymoron, in University of Chicago Law Review, 2003,

[52] Sui limiti del nudging cfr. S. BALDWIN, From regulation to behaviour change, London School of Economics, 2014.

entra in tensione con le logiche di personalizzazione che costituiscono il fondamento del *business model* delle principali piattaforme digitali.

La letteratura economica ha evidenziato come la personalizzazione algoritmica, pur migliorando l'efficienza allocativa attraverso il *preference matching*, possa generare forme di discriminazione indiretta (*disparate impact*) che colpiscono gruppi sociali vulnerabili[53]. Il *statistical discrimination* basato su correlazioni statistiche tra caratteristiche demografiche e comportamenti può, inoltre, perpetuare e amplificare pregiudizi sociali preesistenti[54].

Il divieto di discriminazione algoritmica configura, così, un vincolo che può ridurre l'efficienza economica complessiva del sistema in nome dell'equità distributiva. Questo trade-off tra efficienza e equità assume particolare rilevanza nel contesto del marketing digitale perchè la personalizzazione rappresenta la fonte principale di valore aggiunto.

La Dichiarazione non fornisce criteri chiari per risolvere questo trade-off, limitandosi a richiedere dataset adeguati senza specificare i parametri di adeguatezza. Si configura perciò uno spazio di discrezionalità tecnico-normativa che rischia di trasferire le scelte valoriali fondamentali dal livello politico a quello tecnocratico[55].

La dottrina giuridica ha iniziato ad elaborare principi per la valutazione della fairness algoritmica, distinguendo tra diverse concezioni di equità: *individual fairness* (trattamento simile per individui simili), *group fairness* (parità di trattamento tra gruppi demografici), *counterfactual fairness* (invarianza rispetto a caratteristiche protette). Tuttavia, queste diverse concezioni possono essere mutuamente incompatibili, rendendo necessarie scelte valoriali che eccedono la dimensione puramente tecnica.

## 5.3 Il marketing comportamentale

Il binomio empowerment/marketing digitale evidenzia le contraddizioni più profonde del paradigma delineato dalla Dichiarazione. Si è visto, infatti, che l'evoluzione del marketing digitale verso tecniche sempre più sofisticate di *behavioral targeting* ha trasformato radicalmente il rapporto tra imprese e consumatori, sostituendo il tradizionale modello del *consumer empowerment* con logiche di *consumer*

---

[53] Cfr. C. DWORK, M. HARDT, T. PITASSI, O. REINGOLD, R. ZEMEL, Fairness through awareness, in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, 2012.

[54] Sul statistical discrimination cfr. E. PHELPS, The statistical theory of racism and sexism, in American Economic Review, 1972

[55] Cfr. F. PASQUALE, The black box society, cit.

*manipulation*.

Le tecniche di marketing comportamentale si basano sull'analisi sistematica dei *big data* comportamentali per identificare pattern predittivi che consentono di influenzare le scelte individuali. L'utilizzo di algoritmi di machine learning per l'analisi dei dati di navigazione, delle interazioni social, dei pattern di acquisto e delle preferenze espresse consente alle piattaforme di costruire profili psicografici dettagliati che abilitano forme di persuasione altamente personalizzate.

La ricerca in *neuromarketing* ha evidenziato come queste tecniche possano bypassare i processi di elaborazione cognitiva consapevole, agendo direttamente sui meccanismi neurali subconsci che governano le decisioni di acquisto. L'utilizzo di tecniche come il *subliminal priming*, l'*emotional contagion*, il *social proof manipulation* e l'*artificial scarcity* configura forme di manipolazione psicologica che compromettono l'autenticità delle scelte individuali[56].

Questo fenomeno assume particolare gravità nel contesto dell'economia dell'attenzione, dove la competizione per la *attention capture* spinge le piattaforme digitali verso tecniche sempre più aggressive di *engagement hacking*. L'utilizzo di *variable ratio reinforcement schedules*, *fear of missing out* (FOMO), *infinite scroll designs* e *notification flooding* configura forme di *digital addiction design* che compromettono il controllo volitivo degli utenti[57].

## 5.4 I dark patterns nell'architettura ingannevole

La dottrina giuridica ha iniziato a sistematizzare queste pratiche attraverso il concetto di *dark patterns* - interfacce progettate per indurre gli utenti a compiere azioni non intenzionali o contrarie ai loro interessi. La tassonomia elaborata da Harry Brignull identifica diverse categorie di dark patterns: *bait and switch*, *roach motel*, *privacy Zuckering*, *price comparison prevention*, *misdirection*, *hidden costs*, *friend spam*, *forced continuity*[58].

L'Autorità Garante della Concorrenza e del Mercato italiana ha adottato una definizione normativa di dark patterns come "pratiche che, sfruttando elementi di design, di struttura, di funzione o di modalità di funzionamento delle interfacce,

[56] Sulle tecniche di manipolazione subconscia cfr. B. SHIV, A. FEDORIKHIN, Heart and mind in conflict, in Journal of Consumer Research, 1999.

[57] Sul digital addiction design cfr. A. ALTER, Irresistible: the rise of addictive technology, Penguin Press, 2017.

[58] Cfr. A. MATHUR, G. ACAR, M. FRIEDMAN, E. LUCHERINI, J. MAYER, M. CHETTY, A. NARAYANAN, Dark patterns at scale, in Proceedings of the ACM on Human-Computer Interaction, 2019.

inducono o sono idonee a indurre il consumatore ad assumere decisioni non consapevoli o indesiderate".

La Dichiarazione europea, invece, non affronta esplicitamente la questione dei dark patterns, ma contiene disposizioni che potrebbero fornire la base normativa per la loro regolazione. L'art. 15, lett. f) che vieta lo "sfruttamento delle vulnerabilità e dei pregiudizi" e l'art. 10 che garantisce il diritto a "informazioni obiettive, trasparenti, facilmente accessibili e affidabili" configurano principi generali che potrebbero essere specificati in senso anti-dark patterns.

Tuttavia, la regolazione dei dark patterns mal si adatta alla regolazione della distinzione tra persuasione legittima e manipolazione illecita. La letteratura economica ha evidenziato come molte tecniche di marketing digitale si collochino in una zona grigia tra questi due estremi, rendendo difficile la definizione di criteri normativi oggettivi[59].

# 6. Implicazioni per il management digitale

## 6.1 La trasformazione del risk management digitale: dall'approccio reattivo al proactive compliance

L'adozione del paradigma europeo della sicurezza digitale comporta una notevole trasformazione delle strategie di *risk management* aziendali. Il tradizionale approccio reattivo alla sicurezza informatica - basato sulla correzione *ex post* delle vulnerabilità - deve cedere il passo a un approccio proattivo che integra la sicurezza nella fase progettuale dei prodotti e servizi digitali.

Questa trasformazione richiede investimenti significativi in *privacy engineering* e *security engineering*, discipline che stanno emergendo come nuove competenze strategiche nel management digitale. La letteratura manageriale ha già evidenziato come l'integrazione della privacy e della sicurezza nella fase progettuale, pur comportando costi iniziali più elevati, generi significativi risparmi nel lungo termine attraverso la riduzione dei costi di conformità e dei rischi reputazionali.

L'implementazione del paradigma *by design* richiede, inoltre, una riorganizzazione dei processi aziendali che integri le competenze legali, tecniche e di business

[59] Cfr. C. SUSSER, R. ROESSLER, H. NISSENBAUM, Technology, autonomy, and Manipulation, in Internet Policy Review, 2019

in team multidisciplinari. Il tradizionale modello di governance *silos-based* - che assegna la responsabilità privacy e sicurezza a funzioni specializzate separate dal core business - si rivela inadeguato per gestire la complessità sistemica del compliance digitale.

Si è iniziato, quindi, a elaborare modelli di *digital governance* che integrano privacy, sicurezza e business strategy in un framework unitario. Il modello del *Privacy and Security by Design* (PbSD) proposto da Ann Cavoukian rappresenta un tentativo di sistematizzazione di questi principi in una metodologia operativa.

## 6.2 La competitive advantage della compliance etica

L'approccio *value-based* delineato dalla Dichiarazione europea può configurare una fonte di vantaggio competitivo per le imprese che sapranno anticipare le aspettative normative e sociali. La ricerca empirica ha dimostrato come i consumatori europei manifestino una crescente *privacy consciousness* che si traduce in preferenze di acquisto orientate verso prodotti e servizi rispettosi della privacy.

L'indagine Eurobarometro 2019 sulla protezione dati ha evidenziato come il 67% dei cittadini europei sia preoccupato per la privacy online e il 59% consideri importante che le aziende adottino pratiche privacy-friendly. L'evoluzione delle preferenze dei consumatori configura un'opportunità di mercato per le imprese che adottano strategie di *privacy-first marketing*.

Le imprese che adotteranno proattivamente i principi della Dichiarazione potranno beneficiare di un *first-mover advantage* nel mercato europeo, configurando la compliance etica come elemento di differenziazione competitiva anzichè come semplice costo di adeguamento normativo. Il caso di Apple, che ha fatto della privacy un elemento distintivo della propria strategia di brand, dimostra come la protezione dati possa essere trasformata da vincolo normativo in fattore di vantaggio competitivo.

È pur vero, però, che questa strategia presenta rischi significativi legati alla *compliance complexity* e ai costi di implementazione. L'adozione di standard privacy e sicurezza superiori a quelli richiesti dalla normativa comporta investimenti in tecnologie, processi e competenze che possono ridurre la competitività nei mercati price-sensitive.

## 6.3 Marketing etico e sustainable engagement

L'emergere del paradigma dell'empowerment digitale sta spingendo alcune imprese verso l'elaborazione di modelli di marketing più rispettosi dell'autonomia

degli utenti. Il concetto di *ethical marketing* non si limita alla compliance normativa, ma abbraccia una visione più ampia che considera l'impatto sociale e psicologico delle strategie commerciali.

Alcune piattaforme digitali hanno iniziato a sperimentare modelli di *sustainable engagement* che privilegiano la qualità dell'interazione rispetto alla massimizzazione del tempo di utilizzo. Iniziative come *time well spent*, *digital wellbeing* e *responsible design* rappresentano tentativi di conciliare le esigenze di business con il benessere degli utenti[60].

Ma questi approcci si scontrano con le logiche strutturali dell'economia digitale, in cui la maggior parte dei ricavi deriva dalla monetizzazione dell'attenzione attraverso la pubblicità comportamentale. La transizione verso modelli di business più rispettosi dell'empowerment degli utenti richiede innovazioni radicali nei meccanismi di *value creation* che ancora non hanno trovato validazione di mercato.

La ricerca accademica ha iniziato ad esplorare modelli alternativi di monetizzazione che potrebbero riconciliare sostenibilità economica e empowerment degli utenti. Modelli basati su subscription, freemium etico, data cooperatives e attention markets rappresentano possibili alternative al paradigma dell'advertising-based surveillance capitalism.

# 7. Le criticità applicative: enforcement, compliance e limiti sistemici

## 7.1 Il problema dell'enforcement

La natura dichiarativa del documento europeo rende difficile la sua efficacia giuridica e i meccanismi di enforcement. L'art. 10 del preambolo chiarisce che la Dichiarazione "ha natura dichiarativa e, come tale, non incide sul contenuto delle norme giuridiche o sulla loro applicazione", configurando il documento come *soft law* privo di efficacia vincolante diretta.

Ciò anche se la giurisprudenza europea ha riconosciuto alle dichiarazioni istituzionali un ruolo interpretativo significativo nella definizione dei principi generali del diritto UE[61]. La Corte di Giustizia ha già utilizzato documenti di soft law per pre-

[60] Cfr. Center for Humane Technology, The ledger of harms, 2018.

[61] Cfr. T. TRIDIMAS, The general principles of EU law, Oxford University Press, 2006

cisare il contenuto di principi costituzionali non scritti e orientare l'interpretazione della normativa derivata.

Nel caso specifico della Dichiarazione sui diritti digitali, l'efficacia normativa indiretta potrebbe manifestarsi attraverso diversi meccanismi: l'interpretazione conforme della normativa esistente (GDPR, DMA, DSA), l'orientamento dell'attività normativa futura della Commissione, l'influenza sui processi di standardizzazione tecnica.

La letteratura giuridica ha evidenziato come la soft law possa configurare una forma di *anticipatory compliance* che spinge gli operatori privati ad adeguarsi ai principi enunciati anche in assenza di obblighi vincolanti. Nel contesto digitale, in cui la regolazione hard law soffre di ritardi strutturali, la soft law può rappresentare uno strumento più agile per orientare i comportamenti degli stakeholder[62].

## 7.2 La complessità della compliance cross-border

L'implementazione dei principi della Dichiarazione presenta problematicità nel contesto dell'economia digitale globalizzata, caratterizzata da catene del valore transnazionali e da una forte concentrazione geografica delle principali piattaforme. Come noto, la maggior parte dei servizi digitali utilizzati dai cittadini europei è fornita da società con sede negli Stati Uniti o in Asia, soggette a ordinamenti giuridici che non riconoscono i principi dell'empowerment digitale.

La frammentazione normativa internazionale in materia di diritti digitali genera rischi di *regulatory arbitrage* e *forum shopping* che possono compromettere l'effettività delle tutele europee. Le piattaforme digitali possono sfruttare le differenze normative tra giurisdizioni per minimizzare i costi di compliance, spostando attività e dati verso paesi con regolazioni meno stringenti.

Il principio di territorialità del GDPR ha rappresentato un tentativo di contrastare questo fenomeno, estendendo l'applicabilità della normativa europea a tutti i trattamenti che riguardano cittadini UE indipendentemente dalla localizzazione del titolare, ma l'efficacia di questo approccio dipende dalla capacità delle autorità europee di esercitare enforcement extraterritoriale che presenta limiti strutturali significativi.

[62] Cfr. D. KERBER, Governance models for the digital economy, in European Law Review, 2019.

## 7.3 I limiti dell'autoregolazione

Di fronte alle difficoltà dell'enforcement pubblico, la governance digitale europea ha fatto crescente ricorso a meccanismi di autoregolazione e co-regolazione che affidano all'industria la definizione e implementazione di standard tecnici. Il Digital Services Act ha istituzionalizzato questo approccio attraverso il meccanismo dei *codes of conduct* e dei *crisis protocols*.

Eppure gli operatori dominanti potrebbero utilizzare i processi di standardizzazione per consolidare la propria posizione di mercato, definendo standard che favoriscono le loro tecnologie proprietarie a scapito di concorrenti e innovatori.

La ricerca empirica sull'autoregolazione digitale ha evidenziato come le industry initiatives tendano a privilegiare soluzioni tecniche che minimizzano i costi di compliance per le imprese *incumbent*, anche quando questo comporta una riduzione dell'efficacia delle tutele per gli utenti.

Nel contesto specifico dell'empowerment digitale, l'autoregolazione presenta, tra l'altro, il rischio aggiuntivo di definire standard che apparentemente tutelano l'autonomia degli utenti ma nella sostanza preservano le pratiche manipolative più redditizie. Il fenomeno del *privacy theater* e del *consent theater* dimostra come l'industria possa sviluppare soluzioni che soddisfano formalmente i requisiti normativi senza modificare sostanzialmente le pratiche commerciali.

# 8. Prospettive evolutive

## 8.1 L'integrazione con il Digital Services Act e il Digital Markets Act

La Dichiarazione sui diritti digitali non può essere interpretata in isolamento, ma deve essere considerata nel contesto più ampio del *Digital Single Market Package* europeo. L'integrazione con il Digital Services Act e il Digital Markets Act configura un ecosistema normativo che tenta di coniugare la tutela dei diritti individuali con la promozione della concorrenza e dell'innovazione.

Il DSA introduce obblighi di trasparenza e accountability per le piattaforme digitali che si allineano con i principi di empowerment della Dichiarazione. In particolare, gli artt. 15 e 27 del DSA impongono alle piattaforme di fornire informazioni sui sistemi di raccomandazione e sui parametri di moderazione dei contenuti, configurando forme di trasparenza algoritmica che abilitano un controllo più consapevole da parte degli utenti.

Il DMA introduce il concetto di *digital gatekeepers* e impone obblighi di interoperabilità e portabilità che potrebbero ridurre i *switching costs* e aumentare il potere contrattuale degli utenti. L'art. 6 del DMA vieta specificamente pratiche che compromettono la libertà di scelta degli utenti, come il bundling forzato di servizi e il self-preferencing.

Si pone, comunque, un problema di definizione di priorità in caso di conflitti tra obiettivi diversi. La tensione tra empowerment degli utenti e promozione della concorrenza può generare gap difficili da risolvere, particolarmente quando le misure pro-competitive richiedono limitazioni alle scelte individuali.

## 8.2 L'esportazione del modello europeo

I principi della Dichiarazione europea potrebbero influenzare significativamente l'evoluzione delle norme globali sui diritti digitali attraverso il meccanismo del *Brussels Effect*. La ricerca di Anu Bradford ha provato come la regolazione europea tenda a diventare de facto standard globale quando coinvolge mercati di grandi dimensioni con normative stringenti[63].

Nel caso specifico dei diritti digitali, l'effetto Bruxelles potrebbe manifestarsi attraverso diversi canali: l'adozione volontaria di standard europei da parte di multinazionali che operano nel mercato UE, l'influenza sui processi di standardizzazione internazionale, l'emulazione da parte di altre giurisdizioni.

Alcuni paesi hanno già iniziato a elaborare framework normativi ispirati al modello europeo. Il *Personal Information Protection Act* cinese e il *Data Protection Act* indiano contengono disposizioni che riflettono principi simili a quelli della Dichiarazione europea, particolarmente per quanto attiene alla protezione dei minori e alla limitazione delle pratiche manipolative.

Comunque, l'esportazione del modello europeo incontra resistenze significative, particolarmente da parte delle giurisdizioni che privilegiano approcci market-based alla governance digitale. Gli Stati Uniti hanno mantenuto un approccio più permissivo alla regolazione del marketing digitale, considerando molte delle pratiche vietate dalla Dichiarazione europea come espressione legittima della libertà commerciale.

[63] Cfr. A. BRADFORD, The brussels effect: how the European Union rules the world, cit.

## 8.3 Sentieri futuri: AI, metaverso e Web3

Lo sviluppo dell'intelligenza artificiale generativa, degli ambienti virtuali immersivi (metaverso) e delle tecnologie blockchain (Web3) richiede un aggiornamento continuo del framework normativo.

L'intelligenza artificiale generativa presenta rischi specifici per l'empowerment degli utenti, particolarmente per quanto attiene alla generazione di contenuti manipolativi e alla personalizzazione estrema dell'esperienza digitale. La capacità dell'AI di generare contenuti testuali, visivi e audio indistinguibili da quelli prodotti da umani pone questioni inedite circa l'autenticità dell'informazione e la manipolazione delle preferenze.

Il metaverso introduce nuove dimensioni di immersività che potrebbero amplificare gli effetti delle tecniche manipolative. La raccolta di dati biometrici e comportamentali in ambienti virtuali consente forme di profilazione psicologica ancora più invasive di quelle attuali.

Le tecnologie Web3, pur promettendo maggiore decentralizzazione e controllo degli utenti sui propri dati, presentano complessità tecniche che potrebbero escludere ampie fasce di popolazione dal godimento effettivo di questi benefici.

# 9. Conclusioni

La Dichiarazione europea sui diritti e principi digitali configura un tentativo ambizioso di elaborazione di una fenomenologia giuridica del digitale che ponga al centro la dignità umana come valore irriducibile. Il paradigma "sicurezza-protezione-responsabilizzazione" rappresenta un modello di sintesi che, pur nelle sue contraddizioni interne, delinea una *terza via* europea alla governance del digitale, alternativa sia al modello liberal-libertario statunitense che a quello autoritario-sorvegliante di matrice orientale.

Certo, l'analisi del binomio empowerment/marketing digitale evidenzia le tensioni più acute di questo paradigma, rivelando come l'aspirazione all'autonomia individuale nell'ecosistema digitale si scontri con logiche commerciali strutturalmente orientate alla manipolazione delle scelte individuali. La sfida principale consiste, quindi, nel tradurre i principi enunciati nella Dichiarazione in strumenti operativi che sappiano conciliare l'empowerment sostanziale degli utenti con la sostenibilità economica dell'ecosistema digitale.

La ricerca giuridica futura dovrà concentrarsi sullo sviluppo di metodologie

per la valutazione empirica dell'empowerment digitale, superando approcci puramente formalistici per abbracciare metriche outcome-based che misurino l'effettivo potere degli individui di controllare la propria esperienza digitale. Solo attraverso una comprensione empiricamente fondata degli effetti delle diverse pratiche commerciali sarà possibile elaborare una disciplina giuridica che realizzi l'aspirazione della Dichiarazione a una trasformazione digitale che mette le persone al centro.

La sfida che si pone all'interprete contemporaneo - giurista, economista o manager - è quella di tradurre questa visione assiologica in strumenti operativi concreti che sappiano preservare l'ispirazione umanistica del progetto europeo senza cadere nelle trappole del tecno-determinismo o del paternalismo digitale.

Il successo di questo progetto dipenderà dalla capacità del sistema europeo di dimostrare che un'economia digitale *value-based* non solo è compatibile con l'innovazione e la competitività economica, ma può costituire un modello più sostenibile e inclusivo per l'intera comunità globale. Solo attraverso un'ermeneutica attenta alle tensioni dialettiche del testo e alle sue implicazioni sistemiche sarà possibile realizzare quella trasformazione digitale che mette le persone al centro che costituisce l'orizzonte ultimo della Dichiarazione europea[219].

N. 3 - 2025 - pp. 112-132

# Il decennio digitale nella sanità "virtuale": il caso del metaverso

**Alessia Palladino**

**Abstract:** La virtualizzazione della realtà sta offrendo l'opportunità, per cittadini, imprese ed enti pubbli-ci, di sperimentare servizi innovativi ed inedite dinamiche socio-economiche, proponendosi come parte integrante della vita quotidiana.
Per tali ragioni, tale tecnologia ben si interseca nel fenomeno della digitalizzazione della Pubblica Amministrazione, che, sulla scorta delle più recenti politiche del PNRR, mira alla realizzazione di servi-zi digitali innovativi, capaci di potenziare la cura del paziente, riducendo le distanze con il cittadino.
Peraltro, la realizzazione di servizi sanitari digitalizzati e la promozione della telemedicina sono obiettivi delle principali politiche europee, compendiate dapprima nella Strategia Digital Compass, e, successivamente, nella Dichiarazione europea sui diritti e i principi digitali per il decennio digitale. Pertanto, il presente contributo mira a fornire articolate riflessioni sul fenomeno del metaverso, al fine di comprendere se tale tecnologia possa perorare gli obiettivi e i principi enucleati nella recente Dichiarazione europea sui diritti e i principi digitali per il decennio digitale.
Dopo aver analizzato tale tecnologia dal punto di vista tecnico, nonché definitorio, si approfondirà l'impatto e le possibili potenzialità applicative, al fine di comprendere se il metaverso possa fungere da tecnologia sostenibile, capace di garantire uno spazio digitale equo, sicuro e protetto per l'accesso ai servizi sanitari; a tal fine, verranno, altresì, analizzati primi progetti sperimentali nazionali. Nondimeno, le riflessioni saranno condotte anche sulle criticità latenti, insistenti nella dialettica pubblico – privato.

The virtualization of reality is offering the opportunity for citizens, businesses and public bodies to experience innovative services and unprecedented socio-economic di-namics, proposing itself as an integral part of daily life.
For these reasons, such technology intersects well with the phenomenon of digitization of public administration, which, on the basis of the most recent policies of the European Recovery Plan, aims at the realization of innovative digital services, capable of enhancing patient care, reducing the distance with the citizen.

Moreover, the implementation of digitized health services and the promotion of telemedicine are objectives of the main European policies, summarized first in the Digital Compass Strategy, and, later, in the European Declaration on Digital Rights and Principles for the Digital Decade. Therefore, this paper aims to provide articulate reflections on the phenomenon of the metaverse in order to understand whether this technology can plead the goals and principles enucleated in the recent European Declaration on Digital Rights and Principles for the Digital Decade.
After analyzing this technology from a technical, as well as a defining point of view, the impact and possible application potential will be explored in order to understand whether the metaverse can serve as a sustainable technology, capable of guaranteeing an equitable, safe and secure digital space for access to health services; to this end, first national experimental projects will be, also, analyzed. Nevertheless, reflections will also be conducted on the latent critical issues, insistent in the public-private dialectic.

**Parole chiave**: Digitalizzazione, Diritti Digitali, Digital Compass, E-Health, Metaverso

**Sommario**. 1. La tutela della salute nel Decennio Digitale. – 2. Il Metaverso come spazio digitale pubblico. Prime sperimentazioni dei servizi sanitari "virtuali". – 3. Brevi riflessioni definitorie sui "Metaversi". – 4. Il Metaverso come nuova frontiera della Telemedicina nel Decennio digitale. – 5. Criticità e limiti dei servizi sanitari digitali nell'era del Metaverso. – 6. Considerazioni conclusive.

# 1. La tutela della salute nel Decennio Digitale

La *virtualizzazione* della realtà sta offrendo l'opportunità per le Pubbliche Amministrazioni di realizzare servizi pubblici innovativi integrati nella vita quotidiana dei cittadini. In particolare, il Metaverso si propone come ultima frontiera dei mondi virtuali (tra i quali può certamente ricondursi anche l'esperienza delle piattaforme *social*)[1], al punto tale da essere stato ritenuto il "*successore di Internet*"[2], per fornire esperienze immersive, espandendo le latitudini sensoriali ed operative[3].

[1] Come narrato in Snow Crash, "chi può abbandona la realtà e sceglie di vivere nel mondo virtuale generato dai computer, dove libertà e piaceri sono limitati solo dall'immaginazione".

[2] D. Di Rosa, F. Rizzi, *Metaverso. Che cos'è e cosa cambierà: piattaforme, applicazioni, sicurezza*, *cit*.

[3] Sull'impatto delle tecnologie emergenti sulla sfera individuale si rinvia a M. Farina, M., *Brevi riflessioni sullo status delle "persone elettroniche"*, in Ircocervo n. 2/2021, pp. 126 ss.; M. N. Campagnoli, M. Farina, T*ec-no-identità? : percorsi, provocazioni e istanze delle nuove s/oggettività*, Key Editore 2022. Si v. anche, per approfondimenti sul rapporto tra diritto e tecnologia, M. Cartabia, "*Nuovi diritti" e leggi imperfette*, in Iustitia, A. LXIX, 2, 2016, p. 170; Z. Bauman, *Modernità liquida*, Roma-Bari, 2023; N. Bostrom, *Superintelligence: Paths, dangers, strategies*, Oxford University Press, 2014.

Il settore sanitario ha da sempre manifestato una pronunciata inclinazione all'integrazione tecnologica nella pratica medica, costituendo uno dei primi e principali servizi pubblici impattato dalle politiche – europee e nazionali – di digitalizzazione della Pubblica Amministrazione[4]: pertanto, le potenzialità d'utilizzo del metaverso[5] ben potrebbero inaugurare una nuova fase dell'innovazione tecnologica in sanità, capace di estendersi a diverse fasi dell'attività sanitaria, nonché della cura del paziente[6].

Sul punto, le politiche sovranazionali per la digitalizzazione[7] dei servizi sanitari hanno ben consolidato il paradigma della «sanità elettronica»[8] (o «E-*health*»)[9], inaugurando finanche il più recente concetto di «sanità potenziale»[10], e dimostrando che il rapporto tra tecnologia e tutela della salute sia in costante evoluzione ed espansione.

Nel complesso, pertanto, accanto alle consolidate tendenze di *datizzazione*[11]

---

[4] In tal senso, M. Farina, *Ambienti, agenti e intelligenze artificiali nella sanità potenziale. Dilemmi etici e giuridici*, Napoli, 2023.

[5] N. Bostrom, *The future of Humanity*, in J. K. Berg Olsen, E. Selinger, S. Riis (a cura di), *New Waves in Philosophy of Technology*, New York, 2009, 186-215.

[6] C. Sarzotti, *L'assistenza sanitaria: cronaca di una riforma mai nata*, in S. Anastasia, P. Gonnella (a cura di), *Inchiesta sulle carceri italiane*, Roma, Carocci, 2002, pp. 109-121.

[7] E. Carloni, *Algoritmi su carta. Politiche di digitalizzazione e trasformazione digitale delle amministrazioni*, in *Diritto pubblico*, 2, 2019, pp. 363-392.

[8] Per approfondimenti: G. Comandé, *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su «interferenze sistematiche»*, in Studi in onore di Davide Messinetti, vol. I, Napoli: p. 2008; C. Rabbito, *Sanità elettronica e diritto. Problemi e prospettive*, Roma 2010; G. Cipriani, A. V., Gaddi, *La sanità elettronica: in attesa di un salutare "resetting"*, in C. Faralli, R. Brighi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell'eHealth*, Torino, 2015; L. De Panfilis, S. Zullo, *Aspetti etici delle applicazioni eHealth*, in C. Faralli, R. Brighi, M. Martoni M. (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura: il paziente europeo protagonista nell'eHealth*, Torino, 2015; P. Tarallo, *Verso e-Health 2020: casi di successo italiani ed esperienze internazionali*, Milano, 2012; M. G. Virone, *Il fascicolo sanitario elettronico: sfide e bilanciamenti fra Semantic Web e diritto alla protezione dei dati personali*, Ariccia 2015.

[9] Per una ricostruzione del processo di digitalizzazione dell'attività amministrativa, cfr. G. Duni, *L'Amministrazione digitale*, Milano, 2008; cfr. anche F. Bassanini, *Twenty years of administrative reform in Italy*, in *Review of Economic Conditions in Italy*, 3, 2009, pp. 369 ss.; E. Carloni, *L'amministrazione aperta. Regole e limiti dell'open Government*, Rimini, 2014; F. Martines, *La digitalizzazione della pubblica amministrazione*, in *Medialaws*, 2, 2018, pp. 146-157; R. Cavallo Perin, D. U. Galetta, (a cura di), *Il diritto dell'Amministrazione Pubblica digitale*, Torino, 2020.

[10] Per approfondimenti, si vedano: M. Farina, *Ambienti, agenti e intelligenze artificiali nella sanità potenziale*, *cit*.; K. Schaapveld, A. M.J. Chorus, R. J.M. Perenboom, *The European health potential: what can we learn from each other?*, in Health Policy, Vol. 33-3, 1995, pp. 205-217; N. Noorbakhsh-Sabet, R. Zand, Y. Zhang, V. Abedi, *Artificial Intelligence Transforms the Future of Health Care*, in The American Journal of Medicine, Vol. 132 (7), 2019, pp. 795-801; E. Gurevich, B. El Hassan, C. El Morr, *Equity within AI systems: What can health leaders expect?*, in Healthcare Management Forum 2023, vol. 36 (2), pp. 119-124.

[11] Si veda, al riguardo, il recente Regolamento sullo spazio europeo dei dati sanitari (EHDS), che costituisce la pietra angolare dell'Unione europea della salute e il primo spazio comune dei dati in ambito sanitario: Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11

del patrimonio informativo pubblico e di corretta *governance* documentale, la modernizzazione del sistema sanitario si amplia anche alla realizzazione di servizi innovativi e universalmente accessibili alla generalità dei pazienti. Tali obiettivi, peraltro, trovano conferma nelle più recenti politiche delineate nel Piano Nazionale di Ripresa e Resilienza (di seguito, «PNRR»)[12], per la realizzazione di servizi digitali innovativi, capaci di accrescere il benessere sociale individuale, potenziare le relazioni di cura, riducendo le distanze con il cittadino.

Nonostante l'assenza di ogni esplicita menzione alla tecnologia del Metaverso, il Piano – e, in particolare, la Missione 6[13] – ha cristallizzato l'importanza della tecnologia come fattore abilitante nuove frontiere della tutela della salute, capace di affrontare in maniera sinergica i più cruciali aspetti connessi alle attività di cura ed assistenza[14], coinvolgendo tanto l'ammodernamento delle risorse strumentali ed infrastrutturali[15], quanto la digitalizzazione del servizio pubblico[16].

---

febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847, consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ:L_202500327.

[12] Il testo del PNRR è disponibile al seguente indirizzo: https://italiadomani.gov.it/it/ home.html.

[13] Come precisato nel Piano (pag. 228), la missione prevede un finanziamento di 19,7 miliardi e si articola in due componenti: (i) reti di prossimità, strutture intermedie e telemedicina per l'assistenza sanitaria territoriale e (ii) Innovazione, ricerca e digitalizzazione del servizio sanitario nazionale. La prima componente si prefigge l'obiettivo di «rafforzare le prestazioni erogate sul territorio grazie al potenziamento e alla creazione di strutture e presidi territoriali (come le Case della Comunità e gli Ospedali di Comunità), il rafforzamento dell'assistenza domiciliare, lo sviluppo della telemedicina e una più efficace integrazione con tutti i servizi socio-sanitari». La Componente 2, invece, mira a consentire «il rinnovamento e l'ammodernamento delle strutture tecnologiche e digitali esistenti, il completamento e la diffusione del Fascicolo Sanitario Elettronico (FSE), una migliore capacità di erogazione e monitoraggio dei Livelli Essenziali di Assistenza (LEA) attraverso più efficaci sistemi informativi. Rilevanti risorse sono destinate anche alla ricerca scientifica e a favorire il trasferimento tecnologico, oltre che a rafforzare le competenze e il capitale umano del SSN anche mediante il potenziamento della formazione del personale». A tali risorse si accompagnano quelle destinate dal «React EU» (*Recovery Assistance for Cohesion and the Territories of Europe*) e dal Fondo Nazionale Complementare. Per approfondimenti, cfr. Piano Nazionale di Ripresa e Resilienza, consultabile all'indirizzo: https://www.governo.it. Primi approfondimenti sul tema in esame, nonché sulle linee di investimento descritte dal piano, sono compiute da N. Posteraro, *Il fascicolo sanitario elettronico*, in V. Bontempi (a cura di), *Lo stato digitale nel PNRR*, Roma, 2022, pp. 187-199.

[14] Si legge infatti (pag. 225): «[…] Tuttavia, la pandemia ha reso ancora più evidenti alcuni aspetti critici di natura strutturale, che in prospettiva potrebbero essere aggravati dall'accresciuta domanda di cure derivante dalle tendenze demografiche, epidemiologiche e sociali in atto». Per approfondimenti cfr. *ex multis* L. Scillitani, *Un secolo "virato"?*, in G. Palmieri (a cura di), *Oltre la pandemia. Società, salute, economia e regole nell'era del post Covid-19*, vol. I, Napoli, 2020, 747-755, nonché L. Scillitani, *Un diritto "virato"? Virus vi repellere licet (oportet)*, in U. Comite, G. Tarantino (a cura di), *Etica, diritto, salute. Prospettive evolutive nello spazio globale*, Napoli, 2021, pp. 285-298.

[15] Tale obiettivo rientra nella Componente 2 - Innovazione, ricerca e digitalizzazione del Servizio sanitario nazionale. Gli investimenti sono dedicati (i) alla sostituzione di 3100 grandi apparecchiature entro la fine del 2024, (ii) all'ultimazione di 280 interventi di digitalizzazione di DEA di I e II livello entro il 2025, nonché (iii) di 109 interventi di antisismica, cui si aggiungono ulteriori 220 interventi finanziati con le risorse del PNC.

[16] Sui vantaggi della sanità digitale, si veda Anitec-Assinform, *Sanità digitale in Italia. Scenario e Azioni innovative*, maggio 2020; Aspen Institute Italia, *Terapie innovative e welfare: un nuovo paradigma*, Roma, luglio 2019; Deloitte, *Prospettive, potenzialità, impatti e modelli dell'Artificial*

Peraltro, la realizzazione di servizi sanitari digitalizzati[17] e la promozione della telemedicina[18] sono obiettivi delle principali politiche europee, compendiate dapprima nella Strategia *Digital Compass*[19], e, successivamente, nella Dichiarazione europea sui diritti e i principi digitali per il decennio digitale[20].

Nel complesso, tali atti contribuiscono sinergicamente a rafforzare il processo di digitalizzazione dei servizi sanitari: per un verso, il Piano mira a ridurre le principali criticità nella fruizione dei servizi pubblici – connesse *(i)* alla disparità territoriale nell'erogazione dei servizi, *(ii)* all'inadeguata integrazione tra servizi ospedalieri, servizi territoriali e servizi sociali; *(iii)* ai tempi di attesa elevati per l'erogazione di alcune prestazioni, nonché *(iv)* a una scarsa capacità di conseguire sinergie nella definizione delle strategie di risposta ai rischi ambientali, climatici e sanitari –,

La Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, invece, enuncia principi generali, che i decisori pubblici dovrebbero attuare per addivenire ad una trasformazione digitale antropocentrica, sostenibile, inclusiva ed accessibile, coerente con l'essenza stessa dell'Unione europea, fondata sui «valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone

*Intelligence in ambito sanitario*, 2019. A livello europeo, meritevole di citazione è la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana (COM(2018) 233 final) del 25 aprile 2018, consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018DC0233.

[17] A. Masucci, *Digitalizzazione dell'amministrazione servizi pubblici online. Lineamenti del disegno normativo*, in *Diritto Pubblico*, 25 (1), 2019, pp. 117-152.

[18] La Comunicazione della Commissione europea sul Digital Compass sottolinea che (paragrafo 2), «La pandemia di COVID-19 ha dimostrato il potenziale e ha spianato la strada a un uso generalizzato della telemedicina innovativa, dell'assistenza a distanza e di soluzioni robotiche atte a proteggere il personale medico e ad aiutare i pazienti a ricevere assistenza a distanza da casa. Le tecnologie digitali possono consentire ai cittadini di monitorare il proprio stato di salute, adattare il loro stile di vita, promuovere l'indipendenza, prevenire le malattie non trasmissibili e migliorare l'efficienza dei fornitori di servizi sanitari e assistenziali e dei sistemi sanitari. Abbinati a competenze digitali adeguate, i cittadini utilizzeranno degli strumenti che li aiuteranno a proseguire una vita professionale attiva man mano che invecchiano, e gli operatori sanitari e i prestatori di assistenza saranno in grado di sfruttare appieno i vantaggi garantiti da soluzioni sanitarie digitalizzate per monitorare e curare i loro pazienti».

[19] Comunicazione della Commissione Al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final, consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021DC0118.

[20] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, (2023/C 23/01), consultabile all'indirizzo https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32023C0123(01).

appartenenti a minoranze» (art. 2 TUE)[21].

Al contempo, il Capitolo II della Dichiarazione, rubricato "Solidarietà e inclusione", riconosce al punto 7, lett. c) il valore dell'accesso ai servizi sanitari e assistenziali digitali, inserendolo nel contesto più ampio dei servizi pubblici digitali. In particolare, sancisce l'impegno delle istituzioni ad «agevolare e sostenere in tutta l'UE un accesso fluido sicuro e interoperabile a servizi pubblici digitali concepiti per soddisfare le esigenze delle persone in modo efficiente, compresi in particolare i servizi sanitari e assistenziali digitali, segnatamente l'accesso alle cartelle cliniche elettroniche».

Alla luce delle più recenti politiche sovranazionali sulla digitalizzazione della tutela della salute, il presente contributo mira a fornire articolate riflessioni sul fenomeno del metaverso, al fine di comprendere se tale tecnologia possa perorare gli obiettivi e i principi enucleati nella recente Dichiarazione europea sui diritti e i principi digitali per il decennio digitale.

Pertanto, dopo aver analizzato tale tecnologia dal punto di vista tecnico, nonché definitorio, si approfondirà l'impatto e le possibili potenzialità applicative, al fine di comprendere se il metaverso possa fungere da tecnologia sostenibile, capace di garantire uno spazio digitale equo, sicuro e protetto per l'accesso ai servizi sanitari; a tal fine, verranno, altresì, analizzati primi progetti sperimentali nazionali. Nondimeno, le riflessioni saranno condotte anche sulle criticità latenti, insistenti nella dialettica pubblico – privato.

## 2. Il Metaverso come spazio digitale pubblico. Prime sperimentazioni dei servizi sanitari "virtuali"

Come si è tentato di delineare in precedenza, il Metaverso si propone come un fenomeno dirompente, capace di integrare ed armonizzare l'ambiente reale e quello digitale, mediante il ricorso a numerose tecnologie abilitanti, come i Big data, l'Intelligenza Artificiale, la Realtà Aumentata, ma anche l'I*nternet of things* e il *cloud* computing[22].

---

[21] L. Cianci, *Dichiarazione europea sui diritti e i principi digitali: quid pluris?,* in Diritto Pubblico Comparato ed Europeo n. 2/2022, pp. 381-390.

[22] M. Ball, *The Metaverse: What It Is, Where to Find it*, e *Who Will Build It*, MatthewBall.vc, 20 gennaio 2020, in https://www.matthewball.vc/all/themetaverse; si veda altresì M. Ball, *The Metaverse: And How It Will Revolutionize Everything*, W.W. Norton, July 2022. Come evidenziato, altresì, in dottrina,

Per tali ragioni, l'impiego del Metaverso in ambito sanitario sembrerebbe ben incarnare gli intenti delineati nella Dichiarazione europea, volti alla costituzione di uno "spazio digitale pubblico" e a garantire un libero accesso ai principali servizi pubblici.
Del resto, tale tecnologia offre molteplici prospettive d'utilizzo: oltre ad ampliare le frontiere dell'assistenza sanitaria, le potenzialità si estendono anche in diversi campi specialistici della medicina, per il potenziamento delle attività di diagnosi e cura; nonché per supportare le attività di formazione dei professionisti sanitari e dei discenti universitari – anche attraverso accordi interuniversitari[23] –, rappresentando casi clinici simulati[24], con pazienti virtuali che rendono l'esperienza dello studente più immersiva[25].

Nella prassi si sono registrate prime applicazioni nel Metaverso nelle attività di diagnosi e cura in ambito sanitario oltre un decennio fa, con il progetto statunitense *Bravemind*[26], uno strumento clinico interattivo basato sulla realtà virtuale (VR) utilizzato per valutare e trattare il disturbo da stress post-traumatico (PTSD) su veterani e reduci di guerra.
Il ricorso a tali tecnologie risulta diffuso nell'ambito della salute mentale[27], per la

"Il metaverso, inoltre, presenta alcune peculiari caratteristiche, come identificate da un autorevole esperto in materia: — è un sistema persistente, ossia non si "resetta" e non finisce, ma continua a funzionare e ad esistere indipendentemente dall'interazione degli utenti; — è sincrono e vivo, nel senso che il metaverso è un'esperienza che prosegue in modo costante e in tempo reale per tutti gli utenti; — non pone limite al numero di utenti collegati contemporaneamente, pur fornendo a ciascun utente un senso di "presenza" individuale e personalizzato: tutti possono partecipare a uno specifico evento o attività all'interno del metaverso, insieme ad altri utenti connessi, nello stesso momento e con una propria autonomia d'azione; — è un sistema con una propria economia funzionante, dal momento che gli utenti, persone fisiche e giuridiche, sono poste nella condizione di poter creare, possedere, investire, vendere ed essere ricompensati per un'ampia gamma di attività che producono "valore" riconosciuto da altri; — si basa sul meccanismo di interoperabilità tra piattaforme di metaverso, mediante la definizione di standard operativi comuni e il trasferimento di dati, asset e contenuti digitali; — è popolato e alimentato da "contenuti" ed "esperienze" creati e gestiti da una sostanzialmente illimitata gamma di contributori, gli utenti connessi al metaverso". M. Piccinali, A. Puccio, S. Vasta, (a cura di), *Il Metaverso. Modelli giuridici e operativi*, Torino, 2023.

[23] Nel maggio 2024 l'IRCCS San Raffaele di Roma ha sottoscritto una Lettera d'Intenti con la Fondazione Med-Or, l'Università Sultan Moulay Slimane del Marocco e l'Università della Giordania, nell'ambito del Progetto "Medical Med Universities". Sul punto, si rinvia alla pagina tematica https://sanraffaele.it/lirccs-san-raffaele-firma-una-lettera-dintenti-con-med-or-luniversita-sultan-moulay-slimane-del-marocco-e-luniversita-della-giordania/.

[24] Occorre precisare che la prima realizzazione di un caso clinico simulato virtualmente risale al 1971. Sul punto, si v. W. Harless, G. Drennon, J. Marxer, J. Root, G. Miller, *Case: a computer-aided simulation of the clinical encounter*, in *J. Med Educ.*, vol.46, 1971, pp. 443-448.

[25] Attraverso l'uso di Microsoft Hololens, la Case Western Reserve University ha sperimentato l'impiego della Mixed Reality per l'apprendimento avanzato dell'anatomia umana https://case.edu/holoanatomy/about.

[26] https://medvr.ict.usc.edu/projects/bravemind.html.

[27] G. Bansal, K. Rajgopal, V. Chamola, Z. Xiong, D. Niyato, *Healthcare in metaverse: a survey on current metaverse applications in healthcare*, in *IEEE Access*, Volume 10, 2022, 119914-119946, doi:10.1109/

riabilitazione cognitiva e fisica, attraverso l'uso di dispositivi VR per il trattamento di pazienti con lesioni cerebrali, quantunque le potenzialità di tale tecnologia siano riscontrabili in molteplici campi specialistici della medicina, come l'oncologia e la medicina d'urgenza[28].

In ambito chirurgico, nondimeno, il metaverso potrebbe diventare un fattore abilitante per la medicina di precisione, grazie alla creazione di *digital twins* e il ricorso alla robotica, per rendere gli interventi più performanti e sempre meno invasivi.

Di recente, significative sono le iniziative già intraprese, a livello regionale, dai distretti sanitari della regione Sardegna.

Un primo progetto mira ad erogare servizi sanitari da remoto nella realtà penitenziaria di Mamone, luogo dal peculiare isolamento (la struttura penitenziaria, infatti, dista 45 minuti di auto dal primo Comune vicino, e ad un'ora e mezza dal capoluogo), compromettendo il diritto alla salute per le persone presenti nella colonia penale a causa della scarsa agevolezza e sostenibilità di eventuali – talvolta vitali – spostamenti[29].

I primi servizi di cura ed assistenza hanno riguardato l'area psichiatrica e fisiatrica; nel complesso, la sperimentazione mira ad innalzare l'efficienza dell'assistenza sanitaria negli istituti correttivi, eliminando gli ingiustificati fattori ostativi, connessi all'isolamento della struttura.

Significativa è, nondimeno, l'iniziativa sperimentale dell'Azienda Ospedaliero-Universitaria (AOU) di Cagliari, che sfruttando il potenziale dei mondi virtuali, ha recentemente lanciato (ricorrendo al provider *Spatial.io*[30]) il primo ospedale virtuale in Italia[31].

Inaugurato il 24 ottobre 2024, questo innovativo servizio sanitario consentirà ai pazienti di accedere a una vasta gamma di prestazioni sanitarie direttamente da casa; per garantire la fruizione generalizzata di tali servizi, essi sono accessibili utilizzando dispositivi *wearable* come *Oculus*, ma anche attraverso semplicemente l'impiego dei dispositivi d'uso corrente, come PC, tablet e smartphone[32].

ACCESS.2022.3219845.

[28] Y. Zeng, L. Zeng, C. Zang, A. Cheng, *The metaverse in cancer care: applications and challenges*, in Asia-Pacific Journal of Oncology Nursing, Volume 9, Issue 12, December 2022, 100111.

[29] https://www.asl3nuoro.it/metaverso-i-detenuti-di-mamone-primi-in-italia-visitati-da-remoto/.

[30] https://www.spatial.io/.

[31] https://www.aoucagliari.it/home/it/visualizza_notizia.page?contentId=NWS137442.

[32] L'applicazione è disponibile all'indirizzo https://www.spatial.io/s/Ospedale-nel-Metaverso-dellAou-

Attualmente, il nuovo ospedale virtuale offre servizi che si allineano agli intenti descritti nella Dichiarazione europea: questi, infatti, offre servizi di consultazione del proprio Fascicolo Sanitario elettronico, nonché taluni rilevanti servizi sanitari (attraverso il *re-indirizzamento* alle pagine istituzionali), come la prenotazione di visite mediche, il pagamento dei ticket sanitari, e finanche il ritiro dei farmaci; l'Azienda Ospedaliera sta valutando, altresì, di ampliare il catalogo dei servizi offerti, allestendo all'uopo un nuovo piano dell'ospedale virtuale, per offrire servizi di cure palliative, terapia del dolore, formazione e molto altro.

L'ospedale virtuale, inoltre, integra le tecnologie immersive con l'intelligenza artificiale: per fornire assistenza ai pazienti – utenti, infatti, è possibile interagire con un'assistente virtuale in 3D chiamata Anna, alla quale è possibile rivolgere una o più domande a scelta, tra quelle messe a disposizione; nell'orario di apertura dell'Ufficio Relazioni con il Pubblico (URP) nel metaverso, inoltre, è possibile richiedere un appuntamento per parlare con un'operatrice.

Queste iniziative si dimostrano certamente pioneristiche, capaci di poter trasformare radicalmente l'erogazione e l'accesso ai servizi sanitari in Italia, ripianando le possibili carenze della sanità territoriale.
A tal fine, risulta necessario soffermarsi sull'effettiva latitudine definitoria ed operativa di tale tecnologia, per comprendere in concreto lo spessore del Metaverso, e valutarne la funzionalità per la tutela dei diritti digitali.

# 3. Brevi riflessioni definitorie sui "Metaversi"

Le prime sperimentazioni sanitarie negli ambienti immersivi virtuali confermano le potenzialità applicative del Metaverso per la realizzazione delle linee programmatiche tratteggiate nella Dichiarazione europea. Tuttavia, tale tecnologia sfugge ad una compiuta definizione e comprensione[33], e talvolta ricade in un'errata omologazione con tecnologie virtuali affini già esistenti, come ad esempio la realtà estesa ("Extended reality" o "XR"), la realtà virtuale ("Virtual Reality", o "VR")[34], la realtà aumentata ("Augmented Reality", o "AR") e mista ("Mixed Rality", "MR") o finanche

di-Cagliari-6f2c59cc23d0d0c2a3d5292?share=1895739676763264962.

[33] S.M. Park, Y.G. Kim, *A Metaverse: Taxonomy, Components, Applications, and Open Challenges*, in *IEEE Access*, X, 2022, pp. 4209-4251.

[34] P. Milgram, F. Kishino, *A taxonomy of mixed reality visual displays*, in *IEICE Transactions on Information and Systems*, E77-D, 1994, no. 12, pp. 1321- 1329.

dei *digital twins*[35], rappresentazioni digitali di oggetti o sistemi fisici[36].

Dal punto di vista tecnico, infatti, le attuali manifestazioni dei mondi virtuali consistono nel ricorso alla realtà virtuale e aumentata, tecnologie sperimentate sin dagli anni Sessanta del secolo scorso. In particolare, già nel 1962, Morton Heilig creò uno dei primissimi sistemi di realtà virtuale, il *Sensorama*[37]; successivamente, nel 1968, Ivan Sutherland sviluppò il primissimo sistema di realtà aumentata, chiamato *Sword of Damocles*[38]. Il merito di Sutherland si ricollega, peraltro, al tentativo di definire la realtà aumentata, che costituirebbe "*un'illusione bidimensionale di un oggetto tridimensionale presentata all'osservatore, che cambia visivamente esattamente come cambierebbe un oggetto reale quando l'utente muove la testa*"[39].
Nel complesso, dunque, la realtà virtuale offre un'esperienza simulata, che riproduce fedelmente la realtà fattuale, ovvero crea una realtà *sintetica* totalmente immaginaria.

Le peculiarità sottese a tali tecnologie consentono, inoltre, di scorgere le profonde differenze tra la realtà virtuale e quella aumentata. Infatti, a differenza della realtà aumentata, nella realtà virtuale sia gli oggetti, sia l'ambiente, sono totalmente *virtualizzati*. La realtà Aumentata (AR), invece, presuppone una coesistenza tra l'ambiente di vita reale e simulato; per l'effetto, essa sovrappone contenuti generati sinteticamente sul mondo reale, aumentando l'ambiente circostante reale. Inoltre, a differenza della realtà virtuale, gli usi più comuni per la Realtà Aumentata sono ancora prevalentemente connessi all'uso di dispositivi mobili (si pensi, ad esempio, al celebre caso *PokemonGo*[40]), ovvero di *wereable* devices (ricorrendo, ad esempio, alle lenti *Hololens* o ai dispositivi creati da *Meta*).

Del resto, come è stato evidenziato nel dibattito scientifico[41], gli stessi tentativi

---

[35] S. Tagliagambe, *Metaverso e gemelli digitali. La nuova alleanza tra reti neurali e artificiali*, Mondadori 2022.

[36] Come precisato anche dalla Commissione europea nella Comunicazione del 2023 "*An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition*", "Virtual worlds are persistent, immersive environments, based on technologies including 3D and extended reality (XR), which make it possible to blend physical and digital worlds in realtime, for a variety of purposes such as designing, making simulations, collaborating, learning, socialising, carrying out transactions or providing entertainment". Per approfondimenti, si v. COM(2023) 442/final, consultabile all'indirizzo https://digital-strategy.ec.europa.eu/it/library/eu-initiative-virtual-worlds-head-start-next-technological-transition.

[37] M.L. Heilig, *Sensorama simulator*, US Patent 3,050,870, 28 August 1962.

[38] I.E. Sutherland, *A head-mounted three-dimensional display*, in *Proceedings of the December 9–11, 1968, Fall Joint Computer Conference, part I*, p. 757–764. (ACM, 1968).

[39] Per una ricostruzione più articolata, si veda R.T. Azuma, *A survey of augmented reality*, in *Presence: teleoperators Virtual Environ*. vol. 6(4), 1997, pp. 355–385.

[40] https://niantic.helpshift.com/hc/it/6-pokemon-go/faq/28-catching-pokemon-in-ar-mode-1712012768/.

[41] Riprendendo le parole di G. Cerrina Ferroni, "Metaverso, dunque, come "meta-realtà", da non

descrittivi del metaverso si espongono a due distinte interpretazioni: per un verso, infatti, il termine "metaverso" può essere impiegato per fare riferimento in senso generale all'*interfaccia*, cioè all'impalcatura strutturale governata da protocolli di sistema e da standard tecnici che garantiscono l'interazione tra le varie tecnologie; per altro verso, invece, il termine coglie la dimensione *atomica* del metaverso, per richiamare i singoli mondi virtuali accessibili.
Le precisazioni sin qui condotte si estendono, parimenti, anche alla categorizzazione stessa del metaverso, tecnologia dalle potenzialità future senz'altro suggestive, che rischia di deviare in incongrue speculazioni, se non opportunamente contestualizzata.

Anzitutto, risulta utile precisare che il metaverso può assumere una duplice dimensione, *i.e.* centralizzata o decentralizzata.
Nel primo caso (modello *centralizzato*), il nucleo gestionale e decisionale è centralizzato e ben definito in capo ad unico soggetto (società, ente, etc.). Pertanto, i metaversi centralizzati tendono a sviluppare tecnologie di accesso proprie, sistemi di gestione degli applicativi e regole di comportamento per gli utenti[42].

Le ricadute di questo scenario sono alquanto importanti. In caso di metaverso centralizzato, infatti, talune attività – come la personalizzazione dell'avatar, dell'ambiente circostante – sono sì consentite, ma risultano *mediate* dalle scelte operate a monte dai provider della piattaforma. Tale sfumatura si coglie sin dalla prima fase di accesso alla piattaforma, ove è richiesto all'utente di aderire – *necessariamente* – ai Termini e Condizioni d'uso della piattaforma: ne consegue, pertanto, che il metaverso – nella dimensione centralizzata – non si propone come un luogo di assoluta ed incontrollata libertà, ma subisce un temperamento volto a garantire in misura generalizzata l'utilizzo pacifico del metaverso e delle attività nel metaverso.

Nei metaversi decentralizzati, basati su registri distribuiti, invece, si registrano differenti dinamiche relazionali e decisionali[43]. Dal punto di vista tecnico, i metaversi decentralizzati si caratterizzano per tre elementi fondamentali, quali il ricorso *(i)* alla tecnologia Blockchain (registri distribuiti)[44], *(ii)* alle DAO (*Decentralized Autono-*

intendersi come un *al-di-là* della materia, quanto di al-di-là del modo in cui la nostra mente, collegata al cervello, intende la materia". Si v. G. Cerrina Ferroni, *Il metaverso tra problemi epistemologici, etici e giuridici*, *cit.*, pp. 20 ss.

[42] Tra i tipi di metaverso esistenti, un esempio di metaverso centralizzato è *Oculus* di Meta, il primo mondo virtuale immersivo a disposizione degli utenti, esplorabile attraverso l'app Horizon e le sue declinazioni Worlds, Venues e Workrooms.

[43] O. Rikken, M. Janssen, Z. Kwee, *The Ins and Outs of Decentralized Autonomous Organizations (Daos)*, in SSRN Electronic Journal, https://doi.org/10.2139/SSRN.3989559, 2021.

[44] Definita, da Goldman Sachs "*the heart of the Metaverse*". La *blockchain*, infatti, sebbene abbia trovato le sue prime e più note applicazioni nel campo della finanza e delle criptovalute (che giocano un ruolo determinante anche nel metaverso), si configura come un sistema decentralizzato di "notarizzazione" di singoli dati: questi possono riguardare le transazioni, ma anche moduli e

*mous Organizations*)[45] e *(iii)* agli NFT (*Non-Fungible Tokens*)[46].

*Decentraland*[47] rappresenta un esempio paradigmatico di metaverso decentralizzato, che consente di comprendere appieno i meccanismi interattivi e di governance. Le decisioni vengono prese attraverso votazioni, che richiedono il raggiungimento di un quorum di voti (cd. *Voter Power*, *VP*); per l'approvazione, invece, è necessaria una maggioranza semplice. A ogni proprietario di criptovalute – o di *NFT* – vengono attribuiti uno o più voti. Ogni voto sarà registrato permanentemente in una blockchain, che garantisce i requisiti di trasparenza e di immodificabilità. Solitamente, i proprietari di terreni (*Land*) mostrano una quantità di voti superiore rispetto ai possessori di altri beni. Ulteriore classificazione, in relazione all'oggetto del metaverso, è quella tra metaversi che integrano esperienze di vario tipo in un'unica piattaforma, e metaversi che offrono temi o servizi specifici.

L'analisi sin qui condotta consente di addivenire a delle prime riflessioni conclusive.
Il metaverso si propone senza dubbio come una tecnologia emergente, quantunque in attesa di piena affermazione ed espansione, distinta dalle altre realtà virtuali. Peraltro, alla luce dei distinti meccanismi di funzionamento, sarebbe più corretto parlare di "*Metaversi*", anziché di "metaverso", giacché le piattaforme che consentono la *virtualizzazione* della realtà sono molteplici, già numerose, quantunque presentino caratteristiche strutturali differenti.

processi, e, una volta inseriti, risultano sostanzialmente immodificabili, corredati anche datazione e geolocalizzazione dell'immissione; eventuali modifiche, peraltro, richiederebbero il consenso di tutti i partecipanti alla catena (i "nodi"). Per approfondimenti sulla tecnologia si rimanda a A. Palladino, *L'equilibrio perduto della "blockchain" tra "platform revolution" e GDPR compliance,* in *MediaLaws* n. 2/2019, pp. 144-158.

[45] V. Buterin, *Ethereum Whitepaper*, 2014, https://ethereum.org/en/whitepaper/.

[46] Come osservato da G.M. Riccio, *Il metaverso e la necessità di superare i dogmi proprietari*, in *Il Diritto di Internet,* n. 2/2023, pp. 233 ss., "Un NFT è bene di natura digitale, creato all'interno di una blockchain: tuttavia, la caratteristica di tali beni è quella di essere non fungibili, attesa anche la loro impossibilità di essere riprodotti".

[47] https://decentraland.org/. Come si ricava dalla descrizione introduttiva della piattaforma, "Decentraland is a world built by YOU where the only limit is your imagination. Create and sell Wearables & Emotes, construct captivating scenes and interactive experiences, or set up a personal space in your own World". Decentraland è un metaverso sviluppato dagli argentini Ari Meilich ed Esteban Ordano a partire dal 2015. La piattaforma però è stata lanciata ufficialmente soltanto nel 2017 Nel complesso, Decentraland si propone come metaverso generalista, che consente di vivere numerose esperienze e fare affari di ogni tipo. Le interazioni sono basate su una criptovaluta di nome MANA, che sfrutta Ethereum come Blockchain. Dal punto di vista tecnico, l'infrastruttura *peer-to-peer* di Decentraland si compone di tre strati differenti. Il primo strato si chiama *Consensus Layer*, ed è utilizzato per tenere traccia dei contenuti, delle proprietà e delle particelle di terreno presenti all'interno della piattaforma. Il secondo è denominato *Land Content Layer*, ed è finalizzato a raccogliere tutti gli asset utilizzati per renderizzare le scene, dagli oggetti alle texture e ai singoli suoni. Il terzo strato, infine, è il cd. Real-Time Layer, deputato alla gestione di tutte le comunicazioni effettuate nel metaverso.

In ogni caso, il metaverso rappresenta senz'altro una frontiera evolutiva dell'innovazione digitale, che cela l'indiscutibile potenziale di rivoluzionare il dominio e gli standard dei servizi digitali[48], specialmente in ambito pubblico. Volgendo l'attenzione al settore sanitario, certamente il modello centralizzato appare più idoneo per poter salvaguardare la salute individuale e collettiva, nonché per offrire servizi universalmente accessibili e fruibili in misura conforme ai principi delineati nella Dichiarazione europea.

# 4. Il Metaverso come nuova frontiera della Telemedicina nel Decennio digitale

L'utilizzo del metaverso in ambito sanitario cela una latente vocazione alla creazione di nuove modalità di erogazione servizi sanitari sempre più vicini al cittadino, disponibili senza limiti di tempi e spazi.
Tale attitudine, del resto, coglie due aspetti salienti delle attuali politiche e *governance* della salute: per un verso, invero, tali tecnologie favoriscono l'emersione e la diffusione dei più moderni paradigmi in ambito sanitario, tra cui senza dubbio l'*empowerment* del paziente assume rilievo centrale[49]. Il *design* tecnologico, infatti, manifesta uno spessore e un'attitudine antropomorfica ed antropocentrica, al fine di collocare il paziente al centro, renderlo costantemente informato e partecipe nel processo decisionale e terapeutico.

Come osservato in precedenza, sebbene le citate politiche nazionali e sovranazionali non esplicitino dettagli sull'impiego del metaverso nel settore sanitario, il suo utilizzo non sembrerebbe precluso, bensì appare integrarsi in modo significativo nell'attuale quadro normativo dei servizi di telemedicina, ritenuta dal PNRR un asse portante del rafforzamento della sanità territoriale e del miglioramento degli standard di cura di cittadini e residenti[50].
Com'è noto, infatti, le attuali prestazioni sanitarie a distanza si esplicano prevalentemente attraverso teleconsulti effettuati in videochiamata (a mezzo pc, tablet o smartphone), manifestando in tal modo una latente predisposizione per l'interazione virtuale; in questo senso, il ricorso al metaverso potrebbe tradursi in un

[48] G. Carullo, *La nozione di servizi digitali: un nuovo paradigma per la pubblica amministrazione*, in *Istituzioni del Federalismo*, vol. 2, 2023, pp. 335-355.

[49] Secondo la World Health Organization (WHO), l'empowerment è un processo attraverso cui gli individui possono acquisire un maggiore controllo sulle decisioni e sulle azioni che riguardano la propria salute

[50] In dettaglio, il Piano si sofferma su tali servizi nell'ambito della prima componente della Missione 6 (M6C1), allo scopo di a) sviluppare la telemedicina e superare la frammentazione e la mancanza di omogeneità dei servizi sanitari offerti sul territorio; b) sviluppare soluzioni di telemedicina avanzate a sostegno dell'assistenza domiciliare.

miglioramento qualitativo di simili prestazioni[51], consentendo al paziente (ma anche al medico) di interagire in modo più immersivo.

Ciononostante, le potenzialità descritte devono necessariamente conciliarsi con una pletora di requisiti di natura tecnico – giuridica.

In primo luogo, confrontando tali auspici con le attuali Linee Guida sulla Telemedicina del 2022[52], il ricorso alla tecnologia per l'assistenza remota è fruibile esclusivamente da parte di quei pazienti ritenuti *eleggibili* dal punto di vista clinico, tecnologico, culturale e di autonomia (o disponibilità di un *caregiver*, qualora necessario) nella fruizione dei servizi di telemedicina. A tal fine, le Linee Guida impongono di condurre una valutazione di idoneità tecnico – attitudinale: il paziente dovrà essere dotato e saper disporre di apparati tecnologici adeguati (ad esempio, *smartphone* con caratteristiche adeguate all'istallazione di specifiche app per la televisita), anche per l'uso degli appositi ***kit*** per la telemedicina.

Tali barriere all'accesso, tuttavia, rischiano di depotenziare l'impiego di tale tecnologia, a causa degli elevati costi per l'acquisto dei visori necessari per garantire quei connotati caratterizzanti di immersività. Pertanto, è possibile delineare due possibili scenari: nel primo caso, qualora anche la dotazione di visori fosse a carico del paziente – utente, si assisterebbe ad una sensibile riduzione dei candidati eleggibili. Conseguenze più favorevoli si individuerebbero nel caso in cui, invece, tali strumenti venissero concepiti come *dispositivi medici*, ovvero inseriti nei cd. ***kit*** per la telemedicina: in tal caso, si potrebbe delineare un ecosistema unico, in cui i dispositivi di rilevamento dei parametri vitali e clinici del paziente siano interconnessi e valutabili in tempo reale nel metaverso; al contempo, ciò richiederebbe una previa valutazione di compatibilità di simili dispositivi, rispetto ai requisiti delineati nel cd. *Sunshine act* italiano[53].

In secondo luogo, volgendo lo sguardo ai servizi minimi che ogni infrastruttura regionale di telemedicina dovrebbe erogare (televisita, teleconsulto/teleconsulenza, telemonitoraggio e teleassistenza), il metaverso dovrebbe *innovare* i servizi di telemedicina, evitando che esso si traduca in una mera alternativa – o peggio,

---

[51] G. Lofaro, *Piattaforma di Telemedicina e Fascicolo Sanitario Elettronico: il raccordo dei flussi informativi per i servizi sanitari digitali alla luce delle nuove linee guida*, in *Amministrativamente*, II, 2023, pp. 892-918.

[52] *Linee Guida Organizzative Contenenti il Modello Digitale per l'Attuazione dell'Assistenza Domiciliare* del 24 maggio 2022, Decreto del Ministero della salute il 29 aprile 2022 (GU Serie Generale n.120 del 24-05-2022).

[53] Legge 31 maggio 2022, n. 62 recante Disposizioni in materia di trasparenza dei rapporti tra le imprese produttrici, i soggetti che operano nel settore della salute e le organizzazioni sanitarie, in G.U., Serie Generale n. 135 del 11 giugno 2022, entrata in vigore il 26 giugno 2022, in https://www.gazzettaufficiale.it/eli/id/2022/06/11/22G00076/sg.

duplicazione – delle modalità di erogazione dei servizi.

Per tali ragioni, proprio per massimizzare l'attitudine immersiva e la capacità di interconnessione, sarebbe auspicabile che i visori – ma il discorso può essere esteso, altresì, a tutti i dispositivi che consentono di sperimentare nuove frontiere dell'immersività – fossero resi disponibili, sì da evitare la predisposizione di consistenti barriere all'ingresso per la fruizione di tali servizi.

La sperimentazione locale condotta nel corso del 2024 dal Comune di Abbadia San Salvatore[54] ben rappresenta un esempio di utilizzo virtuoso della tecnologia del metaverso, per l'abbattimento di quelle barriere (economiche, sociali, logistiche) che impediscono l'accesso immediato ai servizi di tutela della propria salute.

Il progetto, che ha coinvolto la Casa della salute locale, consente al paziente di accedere ad una pletora di servizi sanitari in modalità remota.

Attraverso l'uso del visore, questi può interagire con gli avatar digitali dei medici oppure partecipare a un corso di attività fisica di gruppo (cd. Afa), a una sessione di fisioterapia, ricevere una consulenza psicologica, nonché condividere attività socioculturali. Nel corso delle sessioni divulgative su tali servizi, inoltre, sono state presentate anche le opportunità per le comunità decentrate create dagli sportelli digitali e dalle televisite.

In sintesi, l'impiego del Metaverso in ambito sanitario ben si concilia con molteplici servizi informativi, assistenziali e diagnostici, ma soprattutto con la morfologia dei servizi di telemedicina, che presuppongono la fisiologica erogazione di servizi a distanza. Tuttavia, l'attuale stato della tecnica rende questa tecnologia fortemente depotenziata, in ragione delle molteplici barriere all'ingresso – soprattutto in termini di costi elevati dei dispositivi – che impediscono di attuare pienamente i principi sanciti dalla Dichiarazione europea e impediscono di attuare una piena sostituibilità delle attuali modalità di erogazione dei servizi.

Sul punto, i servizi di telemedicina risultano emblematici: se, per un verso, l'aterritorialità del Metaverso ben si concilia con le modalità di prestazione dei servizi di telemedicina, per altro verso il necessario ricorso ai *devices* (visori, sensori, etc.) rischia di rendere il servizio meno fungibile, rispetto alle tradizionali modalità. Peraltro, le criticità si acuiscono, qualora tali dotazioni strumentali risultassero a carico dei pazienti – utenti.

Ne consegue, in definitiva, l'esigenza di ponderare l'utilizzo di tale tecnologia, rispetto agli effettivi benefici per la tutela della salute individuale e collettiva.

---

[54] https://www.uslsudest.toscana.it/comunicati-stampa/siena-casa-della-comunita-di-abbadia-san-salvatore-approvato-il-progetto-esecutivo.

# 5. Criticità e limiti dei servizi sanitari digitali nell'era del Metaverso

Il Metaverso e i mondi virtuali presentano molteplici potenzialità tecniche, rilevanti per la realizzazione di ambienti digitali sanitari. Ciononostante, è necessario valutare esattamente le effettive caratteristiche di tali tecnologie, per comprenderne i vantaggi e la concreta capacità di implementare gli obiettivi delineati a livello europeo per la realizzazione di servizi digitali equi, inclusivi ed accessibili. Pertanto, occorre altresì condurre opportune riflessioni su un secondo – ma non secondario, bensì complementare – aspetto di meditazione, che insiste sulla dialettica pubblico – privato[55].

Per quanto il fenomeno del Metaverso sembri diffondersi a livello sperimentale nel settore pubblico[56], per il lancio di innovativi servizi digitali[57], attualmente la maggior parte dei mondi virtuali manifesta natura privata, proprietaria, e dimensione centralizzata, con una tendenza di mercato quasi monopolistica.

Si assiste, dunque, ad un "*feudalesimo del metaverso*", dove le singole piattaforme appaiono come singole proprietà feudali, al cui interno si esplicano le attività sociali ed economiche della comunità che ve ne partecipa.

Tale riflessione reca con sé alcune consequenziali implicazioni.

Anzitutto, un primo aspetto si ricollega alle modalità di accesso e permanenza all'interno dell'ecosistema digitale.

I *provider* privati (in modo non dissimile dalle piattaforme *social*) dispongono di un ampio potere in ordine alla rimozione di utenti, ovvero degli stessi *digital asset* generati o acquisiti dagli stessi in caso di violazione degli standard determinati, unilateralmente, dalla piattaforma stessa[58].

---

[55] I. Pupolizio, *Pubblico e privato. Teoria e storia di una grande dicotomia*, Torino, 2019.

[56] Si pensi, a mero titolo esemplificativo, che anche il Vaticano, attraverso la Fondazione Humanity 2.0, sta sviluppando con Sensorium-Galaxy per rendere fruibili le proprie opere in una nuova galleria di VR9. L'utilizzo della tecnologia si è diffuso anche in Corea del Sud per finalità politiche, propagandistiche; in dettaglio, è stato ricreato nel metaverso lo sbarco a Incheon, episodio rilevante della guerra di Corea.

[57] G. Carullo, *cit*.

[58] A titolo meramente esemplificativo, nelle condizioni generali di utilizzo di The Sandbox, al paragrafo denominato "*Land*", si nota che "You may purchase Lands within The Sandbox. Within your Land, you may edit your Metadata to adjust title, description, URL link, preview image, and logo. All Metadata (and any URL, images, or logos to which it links or that are uploaded) must comply with these Terms and specifically cannot link to or contain any material or content that is pornographic, threatening, harassing, libelous, hate-oriented, harmful, defamatory, racist, xenophobic, or illegal. We reserve the right to moderate and/or delete any Metadata that does not comply with these Terms".

Certamente, ciò non costituisce una assoluta novità nel panorama della *platform economy*: a ben vedere, in effetti, le stesse Condizioni generali d'uso del metaverso (cd. *Terms and Conditions*)[59] risultano sensibilmente modellate su quelle già in uso da parte delle grandi piattaforme esistenti (soprattutto *social*). Queste, infatti, si riservano talune prerogative sui contenuti generati dagli utenti e, parimenti, prevedono regole per l'esclusione o la sospensione degli utenti, ivi comprese le *policy* della piattaforma.

Pertanto, se è pur vero che il metaverso si propone come una nuova frontiera per il potenziamento della salute e per la promozione di servizi digitali innovativi, al contempo si osserva una forte eterointegrazione privata; e talvolta, maggiori spazi di libertà sono il frutto di una attività negoziale.

I *provider*, infatti, consentono ai propri utenti di personalizzare i propri avatar con ulteriori accessori (inclusi copricapi, occhiali, ornamenti e zaini), ornamenti che possono essere acquisiti completando missioni o prove nel metaverso, o acquistati utilizzando valuta virtuale.

Grazie all'integrazione tecnologica con gli strumenti di Intelligenza artificiale[60], gli utenti possono anche personalizzare le qualità vocali e gli elementi audio dei propri avatar e dello scenario circostante, caratteristica particolarmente rilevante per personalizzare la propria esperienza immersiva, imprimendo a questa un carattere distintivo, rispetto alla massa digitale.

Peraltro, alcune piattaforme consentono agli utenti (spesso attraverso dedicati piani di abbonamento) di impostare specifiche attività, ovvero caratterizzare univocamente l'animazione delle loro rappresentazioni virtuali, compresi i movimenti, i gesti e le espressioni facciali, funzionalità capaci di veicolare emozioni, ma altresì di potenziare la capacità interattiva ed identitaria dell'utente nel metaverso.

Del pari, sempre più di frequente gli algoritmi di intelligenza artificiale concorrono alla creazione di ambienti complessi, che (cor-)rispondono dinamicamente alle azioni dell'utente, creando un senso di immersione e coinvolgimento[61].

---

[59] U. Ruffolo, *Piattaforme e content moderation nella dialettica tra libertà di espressione ed autonomia privata*, in European Journal of Privacy Law & Technologies, n.1/2023, pp. 9 ss.

[60] Per approfondimenti si rinvia a L. Corso, *Intelligenza collettiva, intelligenza artificiale e principio democratico*, in *Il diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano 2022, pp. 443 ss.; si v. anche J. Kaplan, *Intelligenza artificiale. Guida al prossimo futuro*, Luiss University Press, 2017, p. 105.

[61] A. C. Mangiameli, *Intelligenza artificiale, big data e nuovi diritti,* in *Rivista Italiana di Informatica e Diritto* n. 1/2022, pp. 93–101.

L'impiego congiunto dell'Intelligenza artificiale consente ulteriori livelli di personalizzazione delle esperienze all'interno del metaverso[62]: l'Intelligenza artificiale analizza i comportamenti, le preferenze e i modelli degli utenti, e riesce ad adattare dinamicamente l'ambiente virtuale, per soddisfare le esigenze individuali. Ciò offre opportunità per esperienze altamente personalizzate, adattate alle specifiche univoche dell'utente.

L'integrazione dell'Intelligenza artificiale nel metaverso, dunque, può consentire la modellazione dei comportamenti dell'avatar, prevedendone le condotte ed anticipandone gli esiti[63].

Ulteriore tema di cui si discorre ancora in modo fievole, ma si pone cruciale rispetto al successo del metaverso, specialmente in ambito pubblico, è quello della interoperabilità dei diversi metaversi, e della portabilità degli avatar e dei *digital assets*.

Infatti, il processo di personalizzazione dell'esperienza è capace di rendere l'esperienza dell'utente più immersiva, e aderente alle sue esigenze; e pertanto, consente di consolidare la propria posizione in un mercato già di per sé contraddistinto da una bassa densità e una forte tendenza monopolistica[64].

Inoltre, questa considerazione cela in sé anche un rischio secondario, associato al controllo privato del metaverso, che consiste nella concentrazione del potere e del controllo nelle mani di poche entità aziendali: in base all'attuale stato di mercato, infatti, il mercato del metaverso presenta scarsa densità, che pertanto alloca il potere decisionale in ambiti non partecipati e ristretti.

Come precisato anche nella recente Risoluzione del Consiglio d'Europa[65],

---

[62] A. Condello, P. Heritier (special issue), , *The Myth of the Law through the Mirror of Humanities. Perspectives on Law, Literature, Psychoanalysis, and Aesthetics*, Law and Literature Volume 33, n. 2/2021, pp. 169 ss.; S. Kasiyanto 2022, *The Legal Conundrums of the Metaverse*, *Journal of Central Banking Law and Institutions*, Vol. 1 No. 2, 2022, pp. 299 - 322, https://jcli-bi.org/index.php/jcli/article/view/25/15.

[63] Studi recenti hanno infatti messo in luce come l'utente umano possa, percepire e avvertire sul proprio corpo l'effetto delle sensazioni del suo avatar (ad esempio provare un senso di vertigine quando l'avatar si trova sull'orlo di un precipizio). Tale fenomeno è noto come "effetto Proteo". Sul punto si rinvia a M. Biasi, *The Labour Side of the Metaverse* (Gli aspetti lavoristici del metaverso), contributo esterno alla rivista *Italian Labour Law e-Journal*, 2023, 16(1), I-X.

[64] Si veda, al riguardo, *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, (a cura di) P. Stanzione, Torino, 2022.

[65] Council of Europe, Resolution 2578 (2024), cit., p. 2. Proprio per tali ragioni, la Risoluzione propone taluni indirizzi operativi per fronteggiare il rischio di monopoli discriminatori (paragrafo 11) "The Assembly is convinced that international co-operation among governments, as well as their collaboration with the private sector and researchers are essential to address the complexities of metaverse technology, promote sound competition and incentivise the development of safe creative

*"Learning from the desktop and mobile era of computing, targeted investment and sound incentives can pave the way for alternatives to the formation of large, concentrated monopolies, exclusionary design, corrosive cultures, and unsustainable production practices. In this respect, the legislative and regulatory framework should consider competition and markets, particularly in relation to distributed monopoly interests spanning hardware, software, content production, publishing, data management, research, advertising and user safety markets".*

Parafrasando le osservazioni sorte anche nel dibattito scientifico[66], gli interessi capitalistici, sottesi alla diffusione e al successo del metaverso, spingono i gestori di tali mondi virtuali a ritrovare nelle esigenze degli utenti il vettore di consolidamento della propria posizione di supremazia gerarchica nel mercato del metaverso.

Tali riflessioni offrono l'occasione per trarre delle prime sintetiche conclusioni.

Il metaverso si propone come un'imperdibile occasione per il conseguimento del benessere economico e sociale nel decennio digitale. Le attuali condizioni, tuttavia, rendono arduo il perseguimento di tali obiettivi, e la realizzazione di una realtà monista, panica.
*È evidente che esiste e continuerà ad esistere una mancanza di interoperabilità tra i vari metaversi, che richiama, per assonanza fenomenica, uno scenario simile a quello dei sistemi operativi dei dispositivi mobili attuali.*

Peraltro, le riflessioni condotte non sembrano subire arresti nel caso di metaversi pubblici. Infatti, quantunque tali tecnologie possono essere utilizzabili anche dagli Enti pubblici, per la diffusione di innovativi servizi, correntemente si assiste alla necessità di esternalizzare la creazione di tali ecosistemi, ricorrendo a soggetti privati per la loro implementazione.

A tal proposito, è opportuno sottolineare che l'esternalizzazione non affievolisce la responsabilità dell'Ente, nell'asseverare le proprie funzioni di garanzia e di tutela dei diritti dei cittadini – utenti.

Pertanto, è auspicabile che i fornitori siano in grado di implementare infrastrutture tecnologiche armonizzate ai principi che regolano la cura degli

immersive ecosystems and ethical metaverse standards. Therefore, the Assembly urges member States to strengthen dialogue and collaboration with business and industry stakeholders, and civil society organisations, with an aim to: 11.1. prevent monopolies and anti-competitive practices; consider limitations to the scale of influence that a single State or a corporate entity may be entitled to accrue across metaverse ecosystems, and create opportunities for new entrants across the metaverse technology stack".

[66] Z. Li, H. Qi, *Platform power: monopolisation and financialisation in the era of big tech*, in *Cambridge J. Econ.*, vol. 46, 2022, pp. 1289–1314. doi: 10.1093/cje/beac054.2022.

interessi pubblici.

Tra i vari, si pensi alle esigenze di garantire, conformemente agli obiettivi delineati nella Dichiarazione europea, (i) l'accesso universale ai servizi pubblici, (ii) adeguati standard di accessibilità, usabilità, pubblicità, trasparenza, equità, (iii) trasparenza dei processi decisionali. Nondimeno, alla luce delle più recenti frontiere della digitalizzazione dell'attività amministrativa, anche il principio di (iv) interoperabilità (alla luce del cosiddetto principio "*Once only*") dovrebbe essere garantito, d'insieme con gli obblighi in materia di (v) protezione dei dati personali e dei diritti fondamentali.

# 6. Considerazioni conclusive

Il presente contributo propone un percorso di riflessioni sulle caratteristiche e sulle dinamiche del metaverso, al fine di valutare in quali termini questi possano effettivamente contribuire alla creazione di innovativi servizi pubblici digitali per la tutela della salute, auspicati dalle più recenti politiche europee per il Decennio Digitale. La riflessione reca con sé ulteriori aspetti, che, muovono dalla ricognizione tecnico – funzionale del Metaverso, nonché della dinamica dei singoli metaversi.

Il quesito ha consentito di valutare, con un approccio globale, aspetti di rilievo primario, come la meccanica del metaverso, la dialettica tra poteri pubblici e soggetti privati, nonché l'effettiva idoneità della tecnologia per lo sviluppo di innovativi servizi digitali.

Nel complesso, il metaverso certamente ripropone questioni e riflessioni comuni all'evoluzione tecnologica e al rapporto tra tecnologia e diritto. A differenza dei precedenti dibattiti, tuttavia, le peculiarità tecniche di tale nuova tecnologia immersiva rendono i termini della questione più articolati, specialmente se simili considerazioni vengono poi "*immerse*" nella sensibile tematica della tutela pubblica della salute.

Al riguardo, la distinzione tra metaversi centralizzati e decentralizzati consente di comprendere che l'esperienza nel metaverso è attualmente frammentata, parcellizzata.

Peraltro, attraverso l'utilizzo dell'intelligenza artificiale, sembrerebbe che l'individuo, piuttosto che esprimere, amplificandola, la propria identità e personalità, spesso si limiti a subire il fascino della *personalizzazione*, fortemente *mediata* ed *eterodeterminata*.

Ciò rischia di confliggere con le esigenze di standardizzazione e di omogenea fruizione dei servizi pubblici. In particolare, il rischio principale risiede nella possibilità di creare differenti metaversi, a seconda della realtà territoriale di riferimento, recando con sé criticità di matrice tecnico – giuridica, che oltre ad insistere sulla necessaria universalità e non discriminazione del servizio, richiede particolari requisiti di accesso per poter far uso di queste tecnologie; nondimeno, la parcellizzazione dei metaversi rischia di tradursi nella impossibilità di interoperabilità, nonché di poter importare il proprio profilo in modo diretto.

Si tratta di un ulteriore tema di cui si discorre ancora in modo molto timido, ma che si pone cruciale rispetto al successo del metaverso, e, a livello globale, rispetto alle suggestioni già manifestatesi sulla possibilità del metaverso di potenziare i servizi pubblici.

Le riflessioni condotte potrebbero risultare affette da profonda miopia, se non fossero collegate al tema della dialettica pubblico – privato, per evitare che l'impiego dei metaversi nel settore pubblico si traduca in una indebita compressione e compromissione dei diritti fondamentali e dei principi che governano l'operato pubblico.

Parimenti, anche l'enforcement regolatorio rappresenta un presupposto indefettibile nella diffusione dei mondi virtuali. Purtuttavia, le attuali spinte regolatorie – seppur ancora raccolte nell'alveo della *soft law* – sembrano ispirarsi prevalentemente (*rectius*, unicamente) alle logiche centralizzate.

In conclusione, l'enforcement regolatorio risulta un aspetto importante per garantire l'uniforme utilizzo ed applicazione di tali tecnologie, conferendo concretezza alle politiche europee e agli obiettivi delineati per il Decennio Digitale.

N. 3 - 2025 - pp. 133-169

# Autori di questo numero

***Matteo Bozzoli***
Junior researcher del Digital Transformation Institute, è coordinatore del gruppo Junior Fellow della Fondazione per la Sostenibilità Digitale.
e-mail: *info@sostenibilitadigitale.it*

***Marco Bussone***
Marco Bussone, 39 anni, giornalista professionista, sposato con un figlio. Dal 2018 Presidente nazionale Uncem e dal 2023 Presidente di PEFC Italia. Consigliere comunale di Vallo Torinese da 10 anni, dal 2020 è Presidente della Fondazione Montagne Italia. Dal 2014 al 2019 è stato Vicepresidente Uncem Piemonte. Autore di diverse pubblicazioni e saggi, ha creato i progetti borghialpini.it e bottegadellalpe.it. Collabora con diverse testate, come Città Nuova, La Voce e il Tempo, il Risveglio. Ha curato il Rapporto Montagne Italia 2025, per Rubbettino, ed è autore della prefazione al libro "Green Community" (Rubbettino Editore).
email: *bussonemarco@gmail.com*

***Enzo Chilelli***
Consulente strategico in ambito Sanità.
Lunga esperienza nel campo dell'informatica pubblica, in particolare nei settori dei trasporti e della sanità. Docente universitario, collabora con le istituzioni in ambito e-health e svolge attività di ricerca applicata e consulenza nel settore sanitario e sociosanitario.
email: *chilelli.enzo61@gmail.com*

***Paolo De Nardis***
Professore emerito di sociologia presso Sapienza, università di Roma, presidente dell'Istituto di studi politici San Pio V, direttore scientifico della "Rivista trimestrale di scienza dell'amministrazione" e di "Studi politici". Già preside della facoltà di sociologia e direttore del dipartimento di Sociologia della Sapienza, è stato membro del consiglio universitario nazionale e ivi presidente del comitato delle scienze politiche e sociali. Ha presieduto il Cattid per l'applicazione delle tecniche di istruzione a distanza in Sapienza.
Ha insegnato anche nelle università di Macerata, Rotterdam, NYU. Autore di oltre 400 pubblicazioni scientifiche.
email: *paolo.denardis@uniroma1.it*

***Stefano Epifani***
Stefano Epifani, presidente del Digital Transformation Institute – Fondazione per la Sostenibilità Digitale, è docente universitario e giornalista. Ha insegnato alla Sapienza di Roma, all'Università di Pavia e in atenei internazionali. Ha collaborato con le Nazioni Unite su progetti di trasformazione digitale e sviluppo urbano sostenibile. Autore del volume Sostenibilità Digitale (2020), è tra i principali esperti italiani di innovazione e sostenibilità, attivo come conferenziere in Italia e all'estero.
email: *info@sostenibilitadigitale.it*

***Massimo Farina***
Professore Associato di Informatica Giuridica presso l'Università degli Studi di Cagliari, già abilitato alle funzioni di Professore di Prima fascia. Avvocato Cassazionista del Foro di Cagliari e Responsabile della protezione dei dati personali (RPD), dell'Ateneo Cagliaritano. Coordinatore del Laboratorio "ICT4Law&Forensics Lab." istituito presso il Dipartimento di Ingegneria Elettrica ed Elettronica, dell'Università degli Studi di Cagliari. Componente del comitato scientifico della Rivista Scientifica della "Rivista Elettronica di Diritto, Economia, Management", diretta dal Prof. Donato A. Limone.
email: *maxfarina@gmail.com*

***Donato Limone***
Già professore ordinario di informatica giuridica; ha insegnato diritto dell'amministrazione digitale e scienza dell'amministrazione digitale; ha insegnato nelle università di Camerino, Luiss, Salento, Federico II Napoli, Sapienza, Unitelma Sapienza; esperto di organizzazione e digitalizzazione delle pubbliche amministrazioni. Fondatore e direttore della "Rivista elettronica di diritto, economia, management".
www.clioedu.it/rivistaelettronica.
email: *donato.limone@gmail.com*

***Andrea Lisi***
Andrea Lisi Avvocato, si occupa di diritto applicato all'informatica da più di 20 anni. Oltre allo Studio Legale Lisi, coordina le realtà di Digitalaw e D&L NET. È il Presidente di ANORC Professioni e il Direttore della Rivista di divulgazione scientifica DIGEAT. Docente universitario e direttore scientifico di Master universitari e percorsi specialistici di settore. È Direttore del Dipartimento DigitaLaw presso CUIRIF - Centro Universitario Internazionale di Ricerca e Innovazione Integral Intelligence. È membro dei quattro Osservatori nati dalla collaborazione tra Oikos Mediterraneo, CNF, Autorità Garante per la protezione dei dati personali e AgID con la Pontificia Università Antonianum. Dal 2024 è iscritto nell'Elenco dei Manager dell'Innovazione gestito da Unioncamere. Con DPCM del 26 gennaio 2023 è stato indicato come Componente del Comitato di Esperti di comprovata esperienza e qualificazione in materia di innovazione tecnologica e transizione digitale della PA per guidare la trasformazione digitale del Paese, ricoprendeo questo ruolo fino a dicembre 2024. É

componente della lista tenuta dal Comitato europeo per la Protezione dei Dati "Experts for the implementation of the EDPB's Support Pool of Experts" relativamente ai settori "Technical expertise in new technologies and information security" e "Legal expertise in new technologies". È componente della Commissione sull'Intelligenza Artificiale dell'Ordine degli Avvocati di Lecce. Riveste il ruolo di Direttore scientifico di numerosi Master e percorsi specialistici di settore, organizzati in collaborazione con Università ed Enti di Formazione nazionali. Attualmente, in qualità di Professore della Pontificia Università Antonianum, è componente di Osservatori istituzionali attivi presso l'Autorità Garante per la protezione dei dati personali, presso l'Agenzia per l'Italia Digitale e presso il Consiglio Nazionale Forense.
email: *andrealisi@studiolegalelisi.it*

***Giovanni Manca***
Ingegnere elettronico esperto di trasformazione digitale e sicurezza informatica. A partire dal 1986 si è occupato di identità digitale, dematerializzazione (conservazione e gestione) dei documenti informatici, sottoscrizioni informatiche, Digital Transaction Management, sicurezza informatica anche applicata al regolamento 679/2016 sulla protezione dei dati personali (GDPR). Nel periodo 1986-1999 ha lavorato in SOGEI per la digitalizzazione del sistema del Catasto, i servizi di rete fino alla messa in linea del primo sito di natura fiscale su Internet. Dal maggio 2001 fino all'aprile 2010 ha svolto attività direttive presso il Centro Tecnico per la RUPA, l'AIPA e il CNIPA. Tali attività hanno riguardato l'accreditamento e controllo delle aziende che operavano come certificatori di firma digitale o come gestori di posta elettronica certificata, il supporto tecnico al legislatore sulle problematiche di trasformazione digitale e la consulenza alle Pubbliche Amministrazioni sull'utilizzo sicuro dei servizi di rete e sulla integrazione nei flussi documentali di strumenti abilitanti come la firma o la PEC. Dal maggio 2010 ha proseguito le attività professionali come consulente in numerose aziende ICT. Dal dicembre 2015 al marzo 2025 ha operato in LAND Srl come Responsabile della formazione, proseguendo le già citate attività di consulenza. Dal 1^ aprile 2025 è Technical Innovation Project Manager con un incarico di esperto presso il Dipartimento della Trasformazione Digitale nell'ambito dell'identità digitale e del regolamento 910/2014. È coautore di norme primarie, come il Codice dell'Amministrazione Digitale, e delle normative tecniche in materia di firma digitale, conservazione documentale e documenti di identità digitale come la Carta Nazionale dei Servizi (CNS) e la CIE (Carta di Identità Elettronica). È docente con attività di alta formazione presso atenei e soggetti privati. Ha pubblicato centinaia di articoli sui temi della trasformazione digitale ed è autore dei libri "Le firme elettroniche" e "Memorie del digitale". È coautore e curatore del libro "Sanità Digitale – Manuale pratico per la gestione di identità, dati e documenti alla luce del regolamento eIDAS". Già Presidente di ANORC (Associazione Nazionale per Operatori e Responsabili della Custodia di contenuti digitali) nel biennio 2016-2018 è stato rieletto per il biennio 2022-2024. Attualmente ricopre la carica di Vice presidente.
email: *mncgnn59@gmail.com*

***Daniele Napoleone***
Tecnologo con oltre trentacinque anni di esperienza nella system integration e nella trasformazione digitale, unisce una solida competenza tecnologica a una profonda comprensione dei processi nei contesti organizzativi e istituzionali in cui opera. Attualmente supporta la Direzione Generale Musei del Ministero della Cultura nella progettazione e governance di programmi complessi in ambito PN *Cultura* e PN *Sicurezza per la legalità*, con un approccio integrato e orientato alla sostenibilità futura delle soluzioni. Coordina team multidisciplinari e multi-fornitore nello sviluppo di sistemi informativi su scala locale, regionale e nazionale, seguendo iniziative che spaziano dalla migrazione e re-architect su cloud PSN alla cybersecurity e compliance normativa, fino all'applicazione di modelli di intelligenza *artificiale nei processi di valorizzazione e tutela del patrimonio culturale*.
Ha ricoperto ruoli di responsabilità in aziende multinazionali e in società italiane di consulenza, realizzando progetti di innovazione in settori eterogenei (energia, telco, finanza, pubblica amministrazione). È promotore di soluzioni pionieristiche per la digitalizzazione della cultura e la gestione dei processi di sicurezza, distinguendosi per la capacità di coniugare innovazione tecnologica, comprensione dei processi e sostenibilità.
email: *daniele.napoleone@gmail.com*

***Alessia Palladino***
Assegnista di ricerca in Informatica Giuridica presso l'Università degli Studi di Cagliari. Dottore di ricerca in «Humanities and technologies: an integrated research path» presso l'Università degli Studi Suor Orsola Benincasa. Master of studies e ELGS Young Researcher presso l'European Public Law Organization (EPLO) di Atene. Specialista in professioni legali presso l'Università degli Studi Suor Orsola Benincasa. Avvocato e Membro di ANDIG (Associazione Nazionale dei Docenti di Informatica Giuridica e di Diritto dell'Informatica).
email: *alessia.palladino@unica.it*

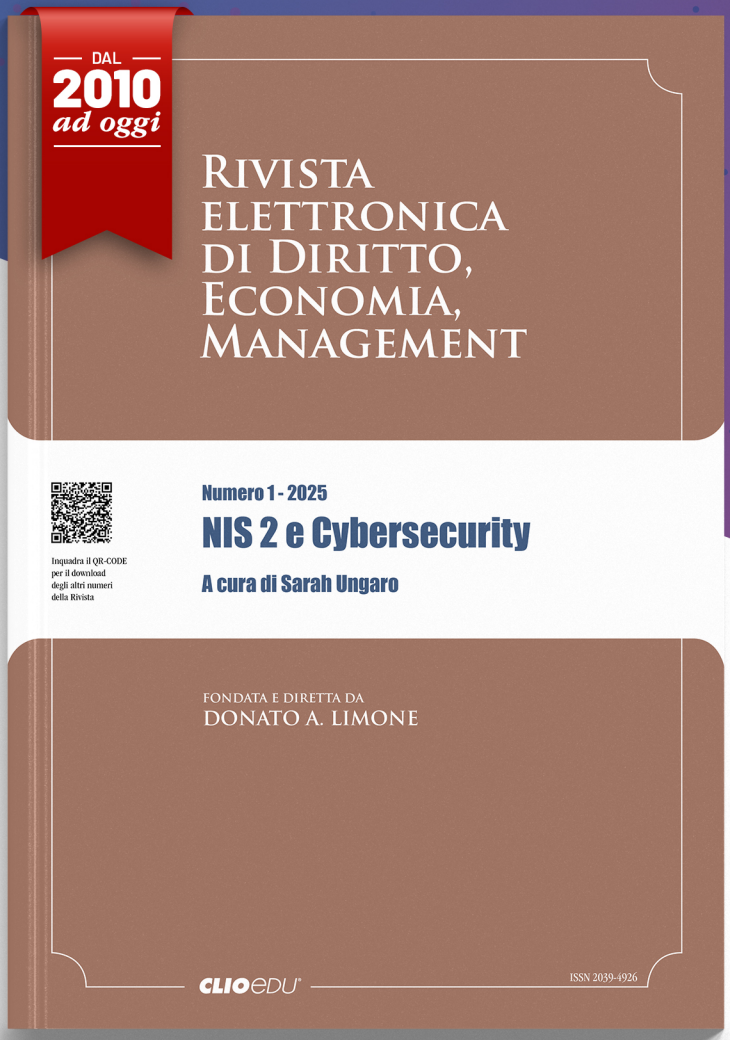
***Enrica Priolo***
Avvocata che opera nel campo delle nuove tecnologie, data protection, criminalità informatica, privacy, sicurezza informatica e infosec; compliance integrata; Intelligenza Artificiale; specializzata in diritti umani e diritto internazionale. Responsabile della protezione dei dati e ODV in aziende private e pubbliche. Formatrice esperta presso numerosi istituti privati e pubblici.
email: *enricapriolo@gmail.com*

***Sarah Ungaro***
Avvocato, dopo la laurea in giurisprudenza conseguita con lode presso l'Università del Salento, ha conseguito il titolo della Scuola di Specializzazione per le professioni legali presso lo stesso Ateneo. Collabora dal 2010 con lo Studio Legale Lisi in qualità di Senior Partner in materia di diritto dell'informatica, protezione dei dati personali,

e-government, contratti IT e cloud, e-health, fascicolo sanitario elettronico, telemedicina, documento informatico, trasparenza amministrativa, open data, riuso, firme elettroniche, dematerializzazione dei documenti contabili e fiscali, conservazione 138 digitale, appalti e e-procurement. In relazione a tali materie, è docente per Università ed enti di formazione specialistica pubblici e privati, partecipa in qualità di relatrice a seminari e convegni. Vicepresidente dell'associazione ANORC Professioni, ne è componente della Commissione di valutazione ed è iscritta nell'Elenco della sezione "Professionisti della digitalizzazione" – Livello Expert e nell'Elenco della sezione "Professionisti della privacy" – Livello Expert, tenuti dalla stessa associazione. Ha partecipato in qualità di autrice alla redazione del Syllabus "Competenze digitali per la PA", il documento realizzato dal Dipartimento della funzione pubblica – Presidenza del Consiglio dei Ministri nell'ambito del progetto "Competenze digitali per la PA" finanziato sul Programma Operativo Nazionale "Governance e capacità istituzionale" 2014-2020 – giunto alla sua seconda edizione (febbraio 2022).È Rappresentante esperto per l'Associazione ANORC all'interno dell'Osservatorio Regionale dell'Agenda Digitale Pugliese. È componente del gruppo di ricerca dell'Osservatorio permanente sulla diplomazia digitale e l'Intelligenza artificiale nato dalla collaborazione tra OIKOS Mediterraneo e la Pontificia Università Antonianum. È componente della Commissione sull'Intelligenza Artificiale dell'Ordine degli Avvocati di Lecce.
email: *sarahungaro@studiolegalelisi.it*

CLIOEDU®

# Soluzioni digitali d'*eccellenza* per progetti di prestigio





FONDATA E DIRETTA DA
## DONATO A. LIMONE

**La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente.**

INQUADRA IL QR-CODE PER IL DOWNLOAD DEGLI ALTRI NUMERI

**www.clioedu.it**/rivistaelettronica

CLIOEDU®