

L'ecosistema digitale europeo tra proclamazione assiologica ed effettività normativa*

Raffaele Torino

Sommario

1. L'ecosistema digitale europeo online come arena regolatoria – 2. La Dichiarazione del 2022 come cornice assiologica – 3. Il principio antropocentrico – 4. La promozione della solidarietà e dell'inclusione nell'ecosistema digitale europeo – 5. La libertà di scelta sostanziale – 6. La partecipazione allo spazio pubblico digitale – 7. La sicurezza e la protezione delle persone – 8. La sostenibilità ambientale e intergenerazionale – 9. Conclusioni: un antropocentrismo prevalentemente reattivo

1. L'ecosistema digitale europeo online come arena regolatoria

L'ecosistema digitale europeo può essere ricostruito, nella sua dimensione economica essenziale, come il mercato dei servizi prestati in rete (online) a favore di utenti stabiliti nel territorio dell'Unione¹. Nel volgere di poco più di un decennio tale mercato ha cessato di essere un comparto specialistico per divenire l'infrastruttura ordinaria dell'esistenza quotidiana di centinaia

* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

¹ Sebbene il termine "ecosistema digitale" indichi, in senso proprio, la totalità dei processi, delle infrastrutture e degli ambienti che operano in formato binario (inclusendo contesti anche del tutto estranei alla connessione in rete, come i sistemi embedded, l'automazione industriale o l'archiviazione locale), lo impiegherò in un'accezione deliberatamente più ristretta. Con "ecosistema digitale" designerò esclusivamente lo spazio online: l'insieme delle piattaforme, dei servizi intermediari, dei sistemi algoritmici e delle infrastrutture di connessione che operano in rete e che il corpus regolatorio europeo esamina e disciplina. Tale restrizione riflette il perimetro applicativo dei regolamenti che saranno oggetto del presente studio, ciascuno dei quali costruisce le proprie figure soggettive (l'interessato, il destinatario del servizio, l'utente finale, la persona esposta a sistemi di IA) in relazione a relazioni che si svolgono, per definizione, in rete, ossia online. In maniera analoga, quando utilizzerò il termine "digitale" mi riferirò alla manifestazione online di tutto ciò che è digitale.

di milioni di persone². Lo spazio digitale è insieme, da una parte, il luogo in cui ci si informa, si formano e si manifestano le opinioni, si intrattengono relazioni sociali, si partecipa al dibattito pubblico e, dall'altra parte, il teatro di un'intensa attività economica, dove il commercio elettronico di beni fisici coesiste con la distribuzione di servizi integralmente smaterializzati. La distinzione tra spazio digitale e spazio analogico, già teoricamente problematica, si è progressivamente attenuata fino a risultare, nella pratica quotidiana, difficilmente percepibile: il digitale online non è più uno strumento tra gli altri, ma la forma prevalente attraverso cui si esercitano le pratiche fondamentali dell'esistenza.

Le dimensioni quantitative di questo ecosistema rendono manifesta la sua rilevanza³. L'analisi per segmenti rivela, in quasi tutte le categorie rilevanti, una concentrazione di potere economico di carattere oligopolistico⁴, finanche antagonista del potere regolatorio pubblico⁵.

I servizi che si svolgono nell'ecosistema digitale sono classificabili in alcune macrocategorie e in ciascuna di esse la struttura del mercato europeo è caratterizzata dalla presenza di uno o pochissimi operatori dominanti, pressoché tutti di origine statunitense. Questi operatori detengono quote di mercato tali da configurare una posizione di *gatekeeper*: controllano l'accesso degli utenti ai servizi e l'accesso dei fornitori terzi agli utenti, definendo unilateralmente le condizioni di un ecosistema che formalmente appartiene al mercato interno europeo, ma che è strutturalmente governato da soggetti che operano secondo logiche e valori radicalmente diversi e che faticano (o semplicemente non vogliono) adeguarsi alle regole europee. Il dato è tanto più significativo se si considera che, come ha sottolineato il Rapporto Draghi del settembre 2024, solo quattro delle prime

² L. Floridi (a cura di), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, 2015.

³ Secondo i dati Eurostat (Eurostat, *Digitalisation in Europe*, ed. 2025, in *ec.europa.eu*, nel 2024 il 93% della popolazione europea ha utilizzato internet; tra gli usi principali figurano la ricerca di informazioni su prodotti e servizi (81%), le comunicazioni vocali e video (79%), l'home banking (72%) e l'accesso a contenuti informativi e social network (circa il 70%). Il 77% degli europei ha effettuato acquisti online e il fatturato generato dalle vendite in rete ha rappresentato il 19% del fatturato totale delle imprese europee.

⁴ K. Kowalski - C. Volpin - Z. Zombori, *Competition in Generative AI and Virtual Worlds*, Competition Policy Brief, 3, September 2024, J. Crémer - Y.A. de Montjoye - H. Schweitzer, *Competition Policy for the Digital Era*, rapporto per la Commissione europea, DG Competition, Lussemburgo, 2019, in *ec.europa.eu*. Per un'analisi sistematica della struttura di mercato delle piattaforme digitali e dei suoi effetti sul benessere degli utenti, v. anche J. Furman et al., *Unlocking Digital Competition. Report of the Digital Competition Expert Panel*, Londra, 2019, Stigler Committee on Digital Platforms, *Final Report*, Chicago, 2019, L.M. Khan, *Amazon's Antitrust Paradox*, *Yale Law Journal*, 126, 2017, 710.

⁵ In argomento, v. O. Pollicino, *Potere digitale*, in M. Cartabia - M. Ruotolo (dir.), *Enciclopedia del diritto*, I Tematici, V-2023, *Potere e Costituzione*, Milano, 2003.

cinquanta imprese tecnologiche mondiali sono europee⁶.

L'asimmetria geopolitica costituita da un mercato da quasi un trilione di euro governato da regole europee⁷, ma servito quasi esclusivamente da imprese statunitensi, costituisce un elemento strutturale di primaria rilevanza al quale l'Unione ha risposto secondo un approccio che si può definire precipuamente europeo: da un lato, disciplinando il fenomeno in conformità ai propri valori e ai propri obiettivi regolatori⁸; dall'altro, cercando di sostenere, nel contesto del mercato interno, le imprese europee del settore e di salvaguardare la risorsa strategica fondamentale di tale mercato, ossia i dati che vengono incessantemente prodotti nell'ecosistema digitale europeo.

Il presente contributo si propone di indagare il primo profilo, ricostruendo e valutando criticamente i valori in base ai quali l'Unione ha disciplinato l'ecosistema digitale online. L'indagine si organizza attorno a due interrogativi che ne guidano lo sviluppo. Il primo riguarda la misura in cui il corpus normativo europeo adottato nell'ultimo decennio ha tradotto i valori proclamati dalla Dichiarazione europea sui diritti e i principi digitali per il decennio digitale del 2022 in posizioni giuridiche soggettive azionabili e standard giurisprudenziali effettivi. Il secondo investe la qualità di questa traduzione e, specificamente, se la risposta regolatoria dell'Unione abbia saputo costruire condizioni positive di autonomia della persona allorché agisce online o si sia limitata a contenere i rischi della tecnologia. La risposta alle due domande, qui anticipata e argomentata nei paragrafi che seguono, è che la giurisdizionalizzazione procede in modo asimmetrico tra i sei valori della Dichiarazione del 2022 e che, sul piano qualitativo, il modello europeo ha sviluppato una postura prevalentemente difensiva che si può definire di *antropocentrismo reattivo*.

L'ipotesi che guida l'analisi è, infatti, che il modello europeo abbia sviluppato una regolamentazione più efficace nel limitare i rischi tecnologici che nel costruire condizioni positive di autonomia della persona e partecipazione democratica.

⁶ M. Draghi, *The Future of European Competitiveness. A Competitiveness Strategy for Europe*, rapporto alla Commissione europea, settembre 2024, 5.

⁷ Per tutti, v. O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete*, in *Rivista AIC*, 2, 2025, 8 aprile 2025, S. Calzolaio - A. Iannuzzi - E. Longo - M. Orofino - F. Pizzetti, *La regolazione europea della società digitale*, Torino, 2024.

⁸ Esula dal presente contributo l'analisi della capacità regolatoria dell'Unione di proiettare i propri standard al di là dei propri confini, definita come *Brussels Effect*, ossia il meccanismo di esportazione involontaria di regole attraverso cui l'Unione eserciterebbe una forma di sovranità regolatoria globale che prescinde dalla giurisdizione formale. In argomento, ovviamente, A. Bradford, *The Brussels Effect. How the European Union Rules the World*, Oxford, 2020, A. Bradford, *Digital Empires. The Global Battle to Regulate Technology*, Oxford, 2023.

Il presente contributo assume i valori proclamati nella Dichiarazione del 2022 non come meri enunciati programmatici, ma come categorie ordinanti utili a testare la coerenza materiale del diritto derivato. L'oggetto dell'analisi non è dunque la validità formale degli atti, bensì la loro capacità di tradurre i valori proclamati in posizioni giuridiche soggettive, obblighi regolatori e standard giurisprudenziali effettivi: il passaggio dalla proclamazione alla giurisdizionalizzazione è il banco di prova su cui si misura la tenuta del modello europeo. L'analisi non si concentrerà sulla struttura delle basi giuridiche degli atti (primariamente l'art. 114 TFUE per il mercato interno e l'art. 16 TFUE per la protezione dei dati) la cui scelta da parte del legislatore dell'Unione pone questioni rilevanti sul piano della competenza e del riparto di poteri, che esulano però dall'obiettivo del presente contributo.

L'esame prende avvio dalla Dichiarazione del 2022, assunta come chiave di lettura dell'architettura normativa (par. 2), per verificare poi la declinazione dei suoi valori nei principali strumenti regolatori. Saranno oggetto di indagine il principio antropocentrico (par. 3), la promozione della solidarietà e dell'inclusione nell'ambito dell'ecosistema digitale europeo (par. 4), la libertà di scelta sostanziale (par. 5), la partecipazione allo spazio pubblico digitale (par. 6), la sicurezza e la protezione delle persone (par. 7), la sostenibilità ambientale e intergenerazionale (par. 8). Il paragrafo conclusivo (par. 9) offre alla discussione un bilancio complessivo del modello regolatorio europeo, individuandone i limiti strutturali e le prospettive evolutive.

2. La Dichiarazione del 2022 come cornice assiologica

Nel dicembre del 2022 il Parlamento europeo, il Consiglio e la Commissione hanno congiuntamente proclamato, in forma interistituzionale, la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale⁹. La Dichiarazione del 2022 si inserisce nel percorso di costruzione di una politica digitale europea dotata di una propria identità valoriale¹⁰, come

⁹ Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, 2022/C 23/01. V., in argomento, P. De Pasquale, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in DUE, 2022, 163; E. Quinn, *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in VBlog, 22 dicembre 2022; P. Passaglia, *La Dichiarazione per la sovranità digitale europea e l'utilità (trascurata) del ricorso alla geopolitica*, in MediaLaws. Rivista di Diritto dei Media, 11 febbraio 2026, 3, 2025, 348.

¹⁰ Tale percorso prende avvio con la Comunicazione della Commissione "Plasmare il futuro digitale dell'Europa" del febbraio 2020 (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final), che ha individuato

complemento assiologico della Bussola per il digitale 2030¹¹, che ha tradotto le priorità strategiche in obiettivi misurabili. La Bussola per il 2020 definisce cosa l'Unione vuole raggiungere, mentre la Dichiarazione del 2022 stabilisce entro quali vincoli valoriali il raggiungimento è da ritenersi legittimo.

La Dichiarazione del 2022 si colloca nella categoria degli strumenti di soft law e non produce obblighi giuridicamente vincolanti per gli Stati membri e per gli operatori privati, né attribuisce diritti soggettivi direttamente azionabili dai singoli. Sarebbe tuttavia superficiale sottovalutarne la portata giuridica, poiché sul piano funzionale essa orienta il legislatore dell'Unione nella definizione delle scelte normative in materia digitale, offre il parametro valoriale rispetto al quale misurare la compatibilità degli atti di diritto derivato, e funge da criterio orientativo ed ermeneutico per l'interprete chiamato a ricostruire la ratio degli obblighi imposti dalla normativa vincolante. Quest'ultima funzione trova conferma esplicita nel sistema delle fonti: l'AI Act stabilisce che le regole armonizzate sui sistemi di intelligenza artificiale «dovrebbero tenere conto della Dichiarazione europea sui diritti e i principi digitali per il decennio digitale» (considerando 7). La Dichiarazione del 2022 opera come meccanismo di vincolo istituzionale del legislatore europeo, ossia una forma di *pre-commitment* valoriale che restringe lo spazio delle scelte normative legittime non sul piano della validità formale, ma su quello della coerenza assiologica¹².

Sebbene non sia invalido, un atto di diritto digitale che si ponga in contrasto con i principi della Dichiarazione del 2022 tradisce la coerenza interna del modello europeo, che ha assunto i valori della Dichiarazione del 2022 come propria identità regolatoria. Sul piano ermeneutico, la Dichiarazione del 2022 ha creato un ambiente interpretativo nel quale quegli stessi valori operano come canoni di lettura degli atti successivi: il giudice chiamato a interpretare una norma in tensione con essi dispone di uno strumento argomentativo per orientarne il significato in senso conforme; l'avvocato generale può farne uso nelle proprie conclusioni; la Commissione può valorizzarli in sede di *enforcement*. Ne deriva una pressione argomentativa crescente sul legislatore, che non è evidentemente una sanzione, ma una forma di *accountability* discorsiva che si esercita negli spazi dell'interpretazione giudiziale, del controllo parlamentare e del dibattito dottrinale. La

nella transizione digitale una delle due priorità strategiche del mandato 2019-2024.

¹¹ 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.

¹² E. Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Oxon, 2023, G. De Gregorio, *The Declaration on European Digital Rights and Principles: A First Analysis from Digital Constitutionalism*, in *The Digital Constitutionalist*, 2 February 2022.

misura in cui questa pressione produca effetti giuridici reali dipende, in ultima analisi, dalla disponibilità della Corte di giustizia a recepire la Dichiarazione del 2022 come criterio ermeneutico rilevante: un passaggio che – come si vedrà – la giurisprudenza non ha ancora compiuto, ma che la logica del sistema valoriale dell’Unione non esclude.

Sul piano testuale, la Dichiarazione del 2022 si articola in sei capitoli corrispondenti ad altrettante aree tematiche: la centralità della persona nella trasformazione digitale; la solidarietà e l’inclusione; la libertà di scelta; la partecipazione allo spazio pubblico digitale; la sicurezza, la protezione e il conferimento di maggiore autonomia e responsabilità; la sostenibilità. L’intero documento è permeato da una centrale ed essenziale concezione antropocentrica secondo la quale la tecnologia deve essere concepita come strumento al servizio dell’essere umano, non come fine in sé, né come variabile indipendente rispetto alla quale il diritto debba soltanto adattarsi. Questa impostazione introduce nella regolazione dell’ecosistema digitale europeo una discontinuità rispetto al paradigma tradizionale del mercato interno, nel quale la liberalizzazione dei servizi è il fine e la tutela dei diritti il suo limite esterno. Tale discontinuità, come si vedrà, non è sempre coerentemente tradotta negli atti di diritto derivato adottati in un arco temporale di circa un decennio.

3. Il principio antropocentrico

Il principio antropocentrico è attuato nell’architettura regolatoria europea in forma prevalentemente difensiva, poiché la persona appare essere tutelata dai rischi della tecnologia più di quanto sia messa nelle condizioni di appropriarsi dei suoi benefici. Questa tensione attraversa il primo capitolo della Dichiarazione del 2022 (“Mettere le persone al centro della trasformazione digitale”), che enuncia il principio fondativo dell’intero sistema valoriale: la tecnologia deve essere al servizio delle persone e andare a loro beneficio¹³, mettendole nelle condizioni di perseguire le proprie aspirazioni «in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali» (art. 1 della Dichiarazione del 2022).

La formulazione del Capitolo I esprime una scelta di metodo prima ancora che di contenuto: il soggetto giuridico di riferimento dell’intero sistema regolatorio non è il mercato, l’innovazione o la tecnologia in sé, ma la persona. Questa impostazione risponde a una precisa opzione teorica che può definirsi di “antropocentrismo regolatorio”, contrapposta tanto al tecnocentrismo (che assume il progresso tecnologico come valore auto-

¹³ L. Floridi et al., *AI4People — An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 689.

mo rispetto al quale il diritto deve adattarsi) quanto al mercato-centrismo (che subordina gli obiettivi e i contenuti della regolazione alle esigenze di efficienza allocativa delle risorse in un libero mercato).

Va sottolineato che il Capitolo I individua nel principio di equivalenza online/offline uno dei pilastri del modello europeo: ciò che è illegale offline è illegale online, e i diritti riconosciuti nell'ambiente fisico devono essere garantiti nell'ambiente digitale senza regressione. Questo principio funziona da clausola generale di estensione dell'intera Carta dei diritti fondamentali dell'Unione europea all'ecosistema digitale online.

In questo contesto, il riferimento più diretto ed esplicito all'antropocentrismo è nell'AI Act¹⁴, che nel considerando 6 enuncia che l'intelligenza artificiale «dovrebbe essere una tecnologia antropocentrica» e «fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani», richiamando esplicitamente la Dichiarazione del 2022 quale riferimento orientativo (considerando 7), e all'art. 1, par. 1, enuncia come scopo del regolamento «promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile»¹⁵. La struttura normativa dell'AI Act incarna questo principio in un sistema a gradazione di rischio: i sistemi di IA che comportano rischi inaccettabili per la dignità, la libertà e i diritti fondamentali sono vietati¹⁶; quelli ad alto rischio sono soggetti a obblighi stringenti di trasparenza, documentazione tecnica e supervisione umana. Pur se precedente alla Dichiarazione del 2022, il GDPR costituisce per molti aspetti l'anticipazione normativa più compiuta dell'antropocentrismo regolatorio e sua componente fondamentale¹⁷. Il considerando 4

¹⁴ 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 (regolamento sull'intelligenza artificiale).

¹⁵ Nell'AI Act il termine ricorre con una frequenza che non ha precedenti nel diritto digitale europeo. Oltre a comparire nell'oggetto del regolamento (art. 1, par. 1) e nel considerando 6, il termine si ritrova anche nel considerando 8, che richiama «l'approccio antropocentrico europeo all'IA», nel considerando 27, che riprende il lessico degli orientamenti etici dell'AI HLEG per un'IA «affidabile ed antropocentrica» e infine nel considerando 176, che replica la formula dell'art. 1 nella clausola di sussidiarietà.

¹⁶ In argomento v. N. Zorzi Galgano, *Il regolamento (UE) 2024/1689 del 13 giugno 2024 sul c.d. alto rischio inaccettabile: le pratiche inerenti sistemi di intelligenza artificiale vietate dal legislatore europeo*, in *Contratto e Impresa*, 1, 2025, 45.

¹⁷ 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).

In realtà, la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati

enuncia con nettezza che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo», mentre il considerando 1 e l'art. 1 del medesimo qualificano la protezione dei dati personali come diritto fondamentale. Fondando la disciplina del trattamento sui diritti azionabili dell'interessato (accesso, rettifica, cancellazione, portabilità, opposizione al trattamento automatizzato), il GDPR ha introdotto nel diritto dell'Unione una concezione personalistica del dato che il Capitolo I della Dichiarazione assume e generalizza¹⁸.

L'ulteriore diritto derivato declina l'antropocentrismo in modo asimmetrico, ciascuno strumento incarnandone una variante distinta. Il DSA¹⁹ lo costruisce come tutela rafforzata del soggetto vulnerabile, vietando la pubblicità profilata nei confronti dei minori e imponendo alle piattaforme di dimensioni molto grandi valutazioni di impatto che riconducono esplicitamente la dignità umana sancita dall'art. 1 della Carta tra i diritti fondamentali da preservare²⁰. Il DMA²¹, di vocazione formalmente concorrenziale, opera sul piano della tutela del contraente debole: la garanzia di mercati equi e contendibili «a vantaggio degli utenti commerciali e degli utenti finali» è il presidio indiretto della centralità della persona contro gli «squilibri gravi in termini di potere contrattuale» imposti dai *gatekeeper*²². Il

personali, nonché alla libera circolazione di tali dati (abrogata dal GDPR con effetto dal 25 maggio 2018) già affermava (considerando 2) che i sistemi di trattamento dei dati «sono al servizio dell'uomo» e che essi «devono, qualunque sia la nazionalità o la residenza delle persone fisiche, rispettare le libertà e i diritti fondamentali delle persone fisiche». L'antropocentrismo del GDPR non è dunque un'innovazione valoriale introdotta nel 2016, ma il consolidamento e l'estensione sistematica di un principio già inscritto nel fondamento genetico del diritto europeo della protezione dei dati. In questa prospettiva, la direttiva 95/46/CE — e non il GDPR — è il vero atto fondativo dell'antropocentrismo regolatorio digitale europeo e la continuità tra i due strumenti sul piano assiologico è più rilevante della discontinuità sul piano tecnico.

¹⁸ Sulla concezione personalistica del dato rimangono fondamentali le riflessioni di S. Rodotà, *Il diritto ad avere diritti*, Bari, 2021, in specie il cap. 12.

¹⁹ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

²⁰ L'art. 28 DSA vieta la pubblicità profilata nei confronti dei minori e impone a tutte le piattaforme misure adeguate e proporzionate a garanzia della loro protezione online; l'art. 34, par. 1, lett. b), obbliga le piattaforme di dimensioni molto grandi a valutare i rischi sistemici per i diritti fondamentali, con riferimento esplicito alla dignità umana sancita dall'art. 1 della Carta dei diritti fondamentali dell'Unione europea.

²¹ 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).

²² L'obiettivo è enunciato dall'art. 1, par. 1 DMA; la descrizione delle pratiche dei gatekeeper come fonte di squilibri contrattuali è del considerando 4.

DGA²³ radica il principio sul piano lessicale: insieme all'AI Act, è l'unico atto in cui il termine "antropocentrico" compare in via testuale (considerando 3), segnando una progressiva sedimentazione del principio nel diritto derivato. L'EMFA²⁴, infine, sposta il baricentro dalla persona-utente alla persona-cittadino: la fruizione di contenuti mediatici pluralistici come «fondamentale per promuovere il dibattito pubblico e la partecipazione civica» trasforma l'antropocentrismo in funzione civica, completando in dimensione partecipativa la tutela individuale prevalente negli altri strumenti.

Sul piano giurisprudenziale, il termine "antropocentrico" non compare in alcuna pronuncia della Corte di giustizia. Eppure la logica antropocentrica percorre in maniera sotterranea le decisioni più rilevanti della corte di Lussemburgo in materia digitale: nelle sentenze relative al diritto all'oblio e al controllo della persona sulla propria sfera informativa online (C-131/12, *Google Spain* (2014)²⁵), ai limiti invalicabili che i diritti fondamentali oppongono alle ragioni di sicurezza nazionale (C-362/14, *Schrems I* (2015); C-311/18, *Schrems II* (2020)²⁶), all'incompatibilità della conservazione generalizzata dei dati con i diritti fondamentali anche in nome della sicurezza nazionale (C-511/18, C-512/18 e C-520/18, *La Quadrature du Net* (2020)²⁷), all'abuso di posizione dominante delle piattaforme nel trattamento dei dati personali a fini pubblicitari (C-252/21, *Meta Platforms* (2023)²⁸), al trattamento massivo di dati dei passeggeri e al principio di pro-

²³ Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

²⁴ Regolamento (UE) 2024/1083 del Parlamento europeo e del Consiglio dell'11 aprile 2024 che istituisce un quadro comune per i servizi di media nell'ambito del mercato interno e che modifica la direttiva 2010/13/UE (regolamento europeo sulla libertà dei media).

²⁵ Su questa pronuncia v. P. de Hert - V. Papakonstantinou, *Google Spain: Addressing Critiques and Misunderstandings One Year Later*, in *Maastricht Journal of European and Comparative Law*, 2015, 624, A. Viglianisi Ferraro, *La Sentenza Google Spain ed il diritto all'oblio nello spazio giuridico europeo*, in *Contratto e Impresa. Europa*, 2015, 159, I. Spiecker genannt Döhmann, *A New Framework for Information Markets: Google Spain*, in *Common Market Law Review*, 2015, 1033, G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. Inf.*, 2014, 591.

²⁶ Sulle pronunce *Schrems v.*, per tutti, C. Gentile, *La saga Schrems e la tutela dei diritti fondamentali*, in *federalismi.it*, 13 gennaio 2021.

²⁷ Su questa pronuncia v. C. Waldron, *French family welfare scoring algorithm challenged by La Quadrature du Net*, in *medialaws.eu*, 4 dicembre 2024.

²⁸ Su questa pronuncia v. P. Manzini, *La nuova anima costituzionale del diritto antitrust europeo*, in *rivista.eurojus.it*, 2025, 440, N. Guggenberger, *Consent as Friction*, in *Boston College Law Rev.*, 66, 2025, 353.

porzionalità (C-817/19, *Ligue des droits humains* (2022)²⁹), e alla tutela contro le decisioni automatizzate (C-203/22, *Dun & Bradstreet* (2025)³⁰), i giudici dell'Unione ragionano sistematicamente sulla centralità della persona come titolare di diritti azionabili nei confronti di soggetti privati dotati di potere strutturale. Ne risulta che il principio è proclamato dal legislatore e praticato dal giudice, ma non ancora formalmente giurisdizionalizzato come tale: un fondamento valoriale in via di consolidamento normativo, ma che non si è ancora tradotto in uno standard interpretativo stabilizzato.

4. La promozione della solidarietà e dell'inclusione nell'ecosistema digitale europeo

La solidarietà digitale emerge nel corpus normativo dell'Unione come valore frammentato, presidiato da strumenti eterogenei che operano con logiche diverse, senza che nessuno di essi costruisca una posizione giuridica individuale pienamente azionabile. La Dichiarazione del 2022 ne definisce il contenuto nel secondo capitolo ("Solidarietà e inclusione"), enunciando il principio secondo cui la tecnologia dovrebbe essere utilizzata per unire le persone, non per dividerle, contribuendo a una società e a un'economia eque e inclusive nell'Unione.

Il nodo concettuale del capitolo è la relazione tra digitalizzazione e disuguaglianza. La Dichiarazione del 2022 prende atto che la trasformazione digitale, abbandonata alla propria logica, tende a riprodurre e amplificare le disuguaglianze preesistenti³¹: chi ha competenze, connettività e risorse trae beneficio dal digitale; chi ne è privo ne resta escluso, subendo al contempo i costi della digitalizzazione dei servizi pubblici e del lavoro. Il principio di solidarietà digitale è, dunque, una risposta normativa a questa tendenza centrifuga, e la sua effettività dipende dalla capacità degli strumenti regolatori di tradurre un impegno politico generale in obblighi concreti e azionabili.

La traduzione normativa del principio è frammentaria, poiché siamo di fronte a tre strumenti, con logiche distinte e nessun raccordo sistemico.

²⁹ Su questa pronuncia v. E. Mendos Kuşkonmaz, *The Grand Gala of PNR Litigations: Case C-817/19, Ligue des droits humains v Conseil des ministres*, in *European Constitutional Law Review*, 19, 2023, 294, J. Gerards, *Machine learning and profiling in the PNR system*, in *VerfBlog*, 8 maggio 2023.

³⁰ Su questa pronuncia v. E. Pandolfi, *Il diritto alla spiegazione nei processi decisionali automatizzati e nei sistemi di intelligenza artificiale: riflessioni a margine della sentenza Dun & Bradstreet Austria*, in *rivista.eurojus.it*, 1, 2026, 269.

³¹ J. van Dijk, *The Digital Divide*, Polity Press, 2020 (2a ed.), N. Couldry - U.A. Meijias, *The Costs of Connection. How Data is Colonizing Human Life and Appropriating It for Capitalism*, Stanford, 2019, J. van Dijk - T. Poell - M. de Waal, *The Platform Society*, New York, 2018.

Sul versante della connettività, il Codice europeo delle comunicazioni elettroniche ha incluso l'accesso a banda larga ad alta velocità nel servizio universale³², integrato dal principio di neutralità della rete sancito dal regolamento (UE) 2015/2120³³ che vieta agli operatori di bloccare o degradare il traffico. Tuttavia, la piena attuazione della Bussola per il digitale 2030 resta largamente incompiuta e il divario di connettività tra aree urbane e rurali persiste come fattore strutturale di esclusione digitale. Sul versante del lavoro, la direttiva (UE) 2024/2831 sul lavoro mediante piattaforme digitali³⁴ ha costruito un minimo statuto protettivo (presunzione legale di subordinazione in presenza di direzione e controllo, trasparenza algoritmica, diritto di contestazione delle decisioni automatizzate, divieto di sorveglianza delle comunicazioni tra lavoratori) la cui ambizione iniziale è stata però significativamente ridotta nel corso dell'iter negoziale, particolarmente sul meccanismo della presunzione. Sul versante dei servizi pubblici digitali, il regolamento (UE) 2024/1183 (eIDAS 2.0³⁵) ha istituito il Portafoglio europeo di identità digitale (EUDI Wallet), che gli Stati membri sono tenuti a rendere disponibile a tutti i cittadini e residenti dell'Unione entro la fine del 2026, garantendo il controllo esclusivo dell'individuo sulla propria identità digitale. La giustapposizione di questi tre dispositivi (connettività universale, statuto del lavoratore di piattaforma, identità digitale) non costruisce un sistema: ciascuno opera su un piano normativo proprio, con destinatari, autorità competenti e meccanismi di tutela disgiunti.

Le dimensioni più trasversali del Capitolo II, ossia la protezione delle persone vulnerabili, la lotta ai bias algoritmici, il contrasto alle discriminazioni digitali, sono trattate da più strumenti contemporaneamente. Tre strumenti convergono nella tutela dei soggetti più esposti. Il GDPR rafforza la disciplina per le categorie particolari di dati ritenute più sensibili dal considerando 51 (art. 9). Il DSA combina la valutazione dei rischi sistemici per gli utenti vulnerabili e i minori con il divieto, valevole per tutte le piattaforme, di pubblicità profilata rivolta a destinatari riconosciuti come minori. Sul

³² Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018 che istituisce il codice europeo delle comunicazioni elettroniche.

³³ Regolamento (UE) 2015/2120 del parlamento europeo e del Consiglio del 25 novembre 2015 che stabilisce misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione.

³⁴ Direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali.

³⁵ Regolamento (UE) 2024/1183 del parlamento europeo e del Consiglio 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.

versante della discriminazione algoritmica, l'AI Act impone ai sistemi ad alto rischio pratiche di governance dei dati che individuino e mitighino le distorsioni in grado di produrre discriminazioni vietate³⁶.

Il quadro complessivo presenta due limiti strutturali. Il primo è l'assenza di attuazione del principio del "*fair share*"³⁷: l'impegno affinché chi trae vantaggio economico dalla trasformazione digitale contribuisca equamente ai costi delle infrastrutture che la rendono possibile è rimasto privo di effetti normativi vincolanti, risolvendosi in un cantiere politico aperto. Il secondo è la frammentazione degli strumenti, poiché la solidarietà digitale è presidiata da regolamenti e direttive che operano con logiche e finalità diverse, senza un coordinamento sistematico che garantisca la coerenza degli esiti verso i soggetti che il Capitolo II intendeva proteggere prioritariamente. La giurisprudenza della Corte di giustizia ha affrontato la logica dell'inclusione senza nominarla come tale. I giudici hanno imposto salvaguardie specifiche contro il rischio di discriminazione indiretta nei sistemi di profilazione algoritmica, riconoscendo che la combinazione di categorie di dati apparentemente neutre può produrre effetti escludenti su gruppi protetti (C-817/19, *Ligue des droits humains* (2022)). In altre pronunce la Corte di Lussemburgo ha rafforzato la tutela individuale contro l'esclusione algoritmica dall'accesso a servizi (C-634/21, *Schufa* (2023)³⁸ e C-203/22, *Dun & Bradstreet* (2025)). Anche in questo ambito, dunque, il principio enunciato dalla Dichiarazione del 2022 attende di essere giurisdizionalizzato come categoria autonoma.

5. La libertà di scelta sostanziale

Nel sistema della Dichiarazione del 2022 la libertà di scelta non designa la mera assenza di coercizione formale, ma la capacità effettiva dell'utente di orientare le proprie decisioni in un ambiente online strutturalmente asimmetrico. Essa è costruita nell'ordinamento digitale europeo attraverso tecniche regolatorie eterogenee: obblighi di trasparenza, divieti di manipo-

³⁶ Si vedano, rispettivamente, l'art. 9 GDPR e il considerando 51 del medesimo regolamento; gli artt. 28, par. 2, 34 e 35 DSA; l'art. 10, parr. 2-3, AI Act, che richiede ai set di dati di addestramento, convalida e prova proprietà statistiche appropriate rispetto ai gruppi di persone cui il sistema è destinato.

³⁷ In argomento v. Z. Warso, *The Limits of The Fair Share Debate*, Open_Future, 6 aprile 2023.

³⁸ Su questa pronuncia v. F. Mattasoglio, *La Corte di giustizia europea, algoritmi e credit scoring. L'apertura del vaso di Pandora delle società che si "limitano" a elaborare gli scoring*, in *Dialoghi di Diritto dell'Economia*, gennaio 2025, F. D'Orazio, *Il credit scoring e l'art. 22 del GDPR al vaglio della Corte di giustizia*, in *Nuova Giur. Comm.*, 2, 2024, 416, A.G. Grasso, *Decisioni automatizzate e merito creditizio: la Corte di giustizia sul credit-scoring*, in *BBTC*, 2024, 715.

lazione, diritti di portabilità, requisiti strutturali di contendibilità. Il nodo concettuale del terzo capitolo della Dichiarazione (“Libertà di scelta”) è la distinzione tra libertà di scelta formale e libertà di scelta sostanziale. Che ogni utente sia formalmente libero di scegliere quale servizio utilizzare è una verità superficiale nell’ambiente online, ma resta il problema è che questa libertà formale è sistematicamente svuotata dalla struttura stessa dell’ambiente digitale, da architetture di interfacce progettate per condizionare le decisioni, da sistemi di raccomandazione che orientano le scelte senza che l’utente ne sia consapevole, da effetti di lock-in che rendono il cambio di servizio costoso o impraticabile, da asimmetrie informative che rendono impossibile un confronto genuino tra alternative³⁹.

La libertà di scelta sostanziale è costruita dal diritto dell’Unione per sottrazione, non per addizione, attraverso divieti di manipolazione, obblighi di trasparenza, diritti di portabilità, ma non strutture positive che garantiscano l’esistenza di alternative effettivamente praticabili. Cinque atti convergono in questa logica con modalità complementari ma con un baricentro comune.

Il GDPR presidia la dimensione consensuale, esigendo che il consenso al trattamento sia libero, specifico, informato e inequivocabile (art. 4, n. 11)⁴⁰ e ritenendolo viziato quando intervenga un significativo squilibrio di potere tra l’interessato e il titolare del trattamento (considerando 43). La portata pratica di questa garanzia è tuttavia ridimensionata dalla circostanza, ormai strutturale, che il consenso al trattamento dei dati personali costituisce frequentemente il presupposto per accedere a servizi o beni digitali⁴¹; consenso che gli utenti pressoché mai negano. Sempre il GDPR, sul versante positivo, riconosce il diritto alla portabilità dei dati (art. 20), che risulta essere strumento concorrenziale tra i pochi a logica abilitante, poiché trasferisce i dati da un titolare all’altro in formato interoperabile, abbassando le barriere al cambio di servizio.

DSA e DMA operano sulle architetture di scelta. L’art. 25 DSA introduce nel diritto dell’Unione il divieto esplicito di dark patterns, prescrivendo che le interfacce online non siano progettate o gestite in modo da «materialmente falsare o compromettere la capacità dei destinatari del servizio

³⁹ In argomento v. D. Susser - B. Roessler - H.F. Nissenbaum, *Online Manipulation: Hidden Influences in a Digital World*, in *Georgetown Law Technology Review*, 4(1), 2019.

⁴⁰ Da ultimo, sulle caratteristiche del valido consenso v. S. Thobani, *Il consenso nella regolazione della circolazione dei dati*, in *Persona e Mercato*, 2, 2025, 469, A.S. D’Amico, *Market Power and the GDPR: Can Consent Given to Dominant Companies Ever Be Freely Given?*, in *European Papers*, 8(2), 2023, 611.

⁴¹ In argomento v. European Data Protection Board, *Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platform*, 17 aprile 2024, P. Gallo, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. Dir. Civ.*, 6, 2022, 1054.

di prendere decisioni libere e informate⁴²». Il DMA estende il divieto ai mercati dominati dai gatekeeper (art. 13, par. 6) e ne completa il presidio con strumenti strutturali (portabilità in tempo reale e interoperabilità (artt. 6 e 7)) che abbattano direttamente le barriere al cambio di servizio. Per i sistemi di raccomandazione, il DSA impone alle piattaforme di dimensioni molto grandi di offrire almeno un'opzione non basata sulla profilazione (art. 38).

Sul piano infrastrutturale, il Data Act⁴³ estende la logica della portabilità ai dati industriali e ai servizi cloud, disciplinando il processo di passaggio tra fornitori in modo tale da neutralizzare gli effetti di lock-in⁴⁴. Infine, l'AI Act presidia la libertà di scelta sul versante delle tecniche manipolative: vieta i sistemi che alterano il comportamento delle persone tramite tecniche subliminali (art. 5)⁴⁵ e impone obblighi di trasparenza nei confronti di chi interagisce direttamente con un sistema di IA (art. 50)⁴⁶.

Il filo che attraversa l'intero capitolo è già visibile nella geometria delle disposizioni richiamate: la libertà di scelta è tutelata prevalentemente per via negativa, attraverso divieti e trasparenza, piuttosto che per via positiva, attraverso costruzione di alternative reali.

La Corte di giustizia ha affrontato i temi della libertà di scelta con crescente nitidezza, senza tuttavia mai elevarla a categoria autonoma. In *Meta Platforms* (C-252/21, 2023), i giudici europei hanno affermato che l'estensione e la pervasività del trattamento dei dati a fini pubblicitari operato da Meta eccede la ragionevole aspettativa degli utenti e non può essere giustificata da un legittimo interesse. In *Schufa* (C-634/21, 2023) e *Dun & Bradstreet* (C-203/22, 2025) i giudici europei hanno riconosciuto che una persona il cui accesso a servizi sia negato sulla base di una valutazione algoritmica

⁴² A. Scaffidi - V. Forte, *Dai dark Patterns agli Hyper-Engaging Dark Patterns: per un'applicazione moderna del divieto ex art. 25 DSA*, in questa *Rivista*, 2, 2025, 431, O. Salvatore, *A proposito dei deceptive design (già dark) patterns*, in G. Grisi - S. Tommasi (a cura di), *Mercato digitale e tutela dei consumatori. Prove di futuro*, Torino, 2024, 63, G. Guerra, *Redesigning Protection for Consumer Autonomy. The case-study of dark patterns in European private law*, Milano, 2023.

⁴³ Regolamento (UE) 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).

⁴⁴ Il diritto al passaggio è garantito dall'art. 25 Data Act, che impone ai fornitori di assicurare l'equivalenza funzionale e la disponibilità dei dati esportabili; l'art. 29 dispone l'abolizione progressiva delle tariffe di passaggio, con eliminazione completa a decorrere dal 2027.

⁴⁵ In argomento v. C. Solinas, *Sistemi di IA e tecniche subliminali, manipolative o ingannevoli. Il perimetro del divieto dell'AI ACT*, in *Contratto e impresa*, 4, 2025, 1018.

⁴⁶ In argomento A. Amidei, *La tutela del consumatore "profilato": obblighi informativi e asimmetrie negoziali*, in *Giur. it.*, febbraio 2025, 461.

opaca non è in condizione di esercitare una scelta informata, né di contestare efficacemente la decisione, e ha imposto ai titolari del trattamento di fornire spiegazioni significative sulla logica dell'automatismo decisionale in forma concisa e intellegibile.

Il quadro che emerge presenta una caratteristica rilevante: la libertà di scelta è tutelata dalla regolazione dell'ecosistema digitale europeo prevalentemente attraverso obblighi di trasparenza e divieti di manipolazione, piuttosto che attraverso diritti positivi di accesso a alternative effettivamente praticabili. Questo approccio rischia di rivelarsi insufficiente in mercati in cui l'alternativa al servizio dominante non esiste o non è accessibile: la trasparenza su come funziona un algoritmo non restituisce libertà di scelta a chi non ha alternative reali. La tensione tra libertà di scelta come diritto individuale e libertà di scelta come condizione strutturale di mercato è il limite che attraversa l'intero Capitolo III della Dichiarazione del 2022.

6. La partecipazione allo spazio pubblico digitale

La partecipazione digitale può a buon titolo collocarsi fra i luoghi di massimo conflitto tra diritti nell'intero corpus normativo europeo: libertà di espressione, tutela del pluralismo e contrasto alla disinformazione si fronteggiano senza che nessuno dei tre valori possa prevalere senza condizionare gli altri. Il quarto capitolo della Dichiarazione ("Partecipazione allo spazio pubblico digitale") ne affronta la dimensione più schiettamente democratica, affermando che ogni persona dovrebbe avere accesso a un ambiente digitale affidabile, diversificato e multilingue; ogni persona ha diritto alla libertà di espressione e di informazione nell'ambiente digitale; le piattaforme online di dimensioni molto grandi dovrebbero sostenere il libero dibattito democratico, attenuare i rischi di disinformazione e tutelare la libertà di espressione.

Il DSA è lo strumento che più direttamente configura gli impegni del quarto capitolo. La sua impostazione normativa riflette consapevolmente la tensione fondamentale, poichè vieta obblighi generali di sorveglianza dei contenuti (art. 8) e tutela la libertà di espressione, garantendo che le decisioni di moderazione siano motivate e contestabili (artt. 16 e 20). Al tempo stesso, impone alle piattaforme di dimensioni molto grandi obblighi stringenti di valutazione e mitigazione dei rischi sistemici per i diritti fondamentali (artt. 34-35), articolati lungo quattro direttrici: contenuti illegali, diritti fondamentali, integrità del dibattito civico e dei processi elettorali, salute pubblica e benessere dei minori⁴⁷. La logica è quella di responsabi-

⁴⁷ L'art. 34, par. 1, DSA individua quattro categorie di rischi sistemici che le piattaforme di dimensioni molto grandi devono valutare: diffusione di contenuti illegali (lett. a); effetti

lizzare le piattaforme per gli effetti sistemici dei loro servizi senza imporre censure preventive sui singoli contenuti.

Sul versante specifico della trasparenza dei sistemi di raccomandazione, il DSA impone a tutte le piattaforme online che vi ricorrono di pubblicare nelle proprie condizioni generali i parametri principali che determinano l'ordine di presentazione dei contenuti e le ragioni della loro importanza relativa (art. 27). Le piattaforme di dimensioni molto grandi sono inoltre tenute a offrire agli utenti almeno un'opzione di sistema non basata sulla profilazione (art. 38). Sullo sfondo di questa architettura normativa emerge una trasformazione qualitativa che il diritto fatica ancora a qualificare e regolare con precisione: le piattaforme di dimensioni molto grandi hanno cessato di essere meri intermediari privati per diventare infrastrutture quasi-pubbliche del discorso democratico⁴⁸. Esse definiscono le condizioni di visibilità dell'informazione, le regole di accesso allo spazio pubblico digitale, i criteri di moderazione del dibattito collettivo, ossia funzioni che nell'ambiente analogico erano proprie delle istituzioni pubbliche o dei media soggetti a obblighi di servizio pubblico. Questa trasformazione è il presupposto implicito del DSA e dell'EMFA, venendo a costituire il fondamento teorico su cui poggia l'intera architettura regolatoria della partecipazione digitale.

Va preso atto che l'accesso alle condizioni di visibilità dell'informazione sono definite unilateralmente da soggetti privati attraverso sistemi algoritmici opachi e incide direttamente sulla qualità dell'appartenenza democratica all'Unione. Chi non raggiunge visibilità nello spazio pubblico digitale è di fatto marginalizzato da quella sfera di partecipazione che le democrazie contemporanee non possono più distinguere dallo spazio pubblico tout court. È su questo piano che la regolazione delle piattaforme cessa di essere materia di diritto del mercato interno e diviene, irrimediabilmente, materia avente un rilievo costituzionale.

L'EMFA interviene nella dimensione istituzionale del quarto capitolo: la libertà e il pluralismo dei media come condizioni costitutive di una democrazia funzionante. Il considerando 2 qualifica la tutela di questi valori come «aspetto essenziale per il buon funzionamento del mercato interno dei servizi di media», riconoscendo in essi pilastri della democrazia e dello Stato di diritto. Il regolamento agisce su tre piani principali: protegge l'indipendenza editoriale dei fornitori di servizi di media da pressioni esterne e governative (artt. 4 e 6); impone la trasparenza sulla struttura proprietaria

negativi sull'esercizio dei diritti fondamentali, inclusi libertà di espressione e pluralismo dei media (lett. b); effetti negativi sul dibattito civico e sui processi elettorali (lett. c); rischi per la salute pubblica, la protezione dei minori e il benessere fisico e mentale della persona (lett. d).

⁴⁸ V. J.M. Balkin, *Free Speech is a Triangle*, in *Columbia Law Review*, 118(7), 2018, 2011.

ria (art. 6, par. 2); disciplina le concentrazioni con impatto significativo sul pluralismo (art. 22).

La relazione tra l'EMFA e il DSA è di complementarità funzionale, poiché il DSA regola le condizioni di distribuzione dei contenuti nelle piattaforme, mentre l'EMFA garantisce le condizioni di produzione e indipendenza dei contenuti giornalistici. Il rischio di lacune normative si colloca nell'intersezione tra i due regolamenti, dove i fornitori di servizi di media accedono agli utenti prevalentemente attraverso le piattaforme soggette al DSA, esponendosi agli effetti dei loro sistemi algoritmici di distribuzione senza che nessuno dei due strumenti affronti compiutamente questa dipendenza di fatto.

La Corte di giustizia ha costruito nel corso di un decennio un corpus coerente in materia di partecipazione al discorso pubblico digitale, articolato attorno al bilanciamento tra libertà di espressione e protezione dei diritti fondamentali. Il filone inaugurato da *Google Spain* (C-131/12 (2014)) ha affermato il diritto alla deindicizzazione come espressione del diritto alla protezione dei dati personali, avviando una giurisprudenza sul bilanciamento tra diritto all'oblio e diritto del pubblico all'informazione che si è consolidata in *Google v. CNIL* (C-507/17 (2019)⁴⁹) e *Google (de-referencing of allegedly inaccurate content)* (C-460/20 (2022)⁵⁰). Sul versante della moderazione dei contenuti, *Glawischnig-Piesczek v. Facebook Ireland* (C-18/18 (2019)⁵¹) ha stabilito che un giudice nazionale può ordinare la rimozione non solo del contenuto dichiarato illecito, ma anche di contenuti identici ed equivalenti, aprendo un problema di compatibilità con il divieto di obbligo generale di sorveglianza che il DSA ha poi tentato di comporre sul piano legislativo. In *Schrems v. Meta Platforms Ireland* (C-446/21 (2024)⁵²), i giudici della Corte di giustizia hanno affermato che il consenso non giustifica il trattamento illimitato di dati personali a fini pubblicitari, incidendo direttamente sulla struttura economica delle piattaforme che finanziano il

⁴⁹ Su questa pronuncia v. F. Balducci Romano, *La Corte di giustizia 'resetta' il diritto all'oblio*, in *federalismi.it*, 5 febbraio 2020.

⁵⁰ Su questa pronuncia v. E. Falletti, *La proiezione della personalità online: quale rapporto tra diritto all'oblio e diffamazione?*, in *Foro it.*, 4, 2023, 188, E. Grillo, *Effettività del diritto alla deindicizzazione: informazioni inesatte e valore informativo delle immagini "thumbnails"*, in *NGCC*, 3, 2023, 546.

⁵¹ Su questa pronuncia v. A. Ricci, *Contenuti illeciti e obblighi «di reazione» del prestatore di servizi di hosting. La Corte di Giustizia interpreta la direttiva 2000/31/CE alla luce del principio di effettività*, in *Giur. comm.*, II, 2020, 1018.

⁵² Su questa pronuncia v. J.A. Cruz, *Schrems v. facebook: Limitations on the Use of Off-Platform Data and Sensitive Personal Data*, in *medialaws.eu*, 28 novembre 2024, O. Pollicino - M. Bassini, *Bridge is Down, Data Truck Can't Get Through... A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, in *The Global Community. Yearbook of International Law and Jurisprudence* 2016, 2017, 254.

discorso pubblico digitale attraverso la profilazione pubblicitaria. Dalla tensione che attraversa l'intero Capitolo IV appare che il modello europeo ha scelto di affrontare i rischi per la democrazia digitale attraverso la responsabilizzazione delle piattaforme e la trasparenza algoritmica, piuttosto che attraverso la regolazione diretta dei contenuti. Questa scelta preserva la libertà di espressione e il divieto di censura preventiva, ma la sua effettività dipende dalla capacità delle piattaforme di valutare genuinamente i rischi sistemici e di mitigarli senza che la mitigazione si traduca a propria volta in forme di controllo privatizzato del discorso pubblico.

7. La sicurezza e la protezione delle persone

La sicurezza è il valore più giurisdizionalizzato dell'intero sistema: nessun altro capitolo della Dichiarazione del 2022 può contare su un corpus giurisprudenziale della Corte di giustizia altrettanto consolidato nel tempo, né su strumenti normativi altrettanto verificati nella prassi applicativa. Il quinto capitolo della Dichiarazione ("Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità") si articola in tre sottosezioni: la sicurezza tecnica di prodotti e infrastrutture; la vita privata e il controllo individuale sui dati; la protezione di bambini e giovani.

Il nodo concettuale del capitolo è la tensione tra sicurezza come valore collettivo (che può giustificare limitazioni alla vita privata in nome della protezione pubblica) e sicurezza come difesa della sfera individuale contro le intrusioni tanto degli attori privati quanto degli Stati. Questa tensione, già presente nella tradizione giuridica europea, si manifesta nel contesto digitale in forme nuove e più acute: la raccolta massiva di dati da parte delle piattaforme⁵³, la sorveglianza di massa da parte dei governi⁵⁴, il tracciamento pervasivo a fini commerciali⁵⁵, l'utilizzo dell'intelligenza artificiale per identificare, classificare e valutare le persone⁵⁶, sono tutti fenomeni che il Capitolo V intende presidiare.

A differenza degli altri valori, la sicurezza è tutelata nel modello europeo in chiave eminentemente infrastrutturale: non per via di diritti soggettivi

⁵³ Su questo tema restano centrali le riflessioni di S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, 2019, S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, S. Rodotà, *Tecnologie e diritti*, Bologna, 1995.

⁵⁴ V. D. Lyon, *Surveillance After Snowden*, Cambridge, 2015.

⁵⁵ V. D. Lyon, *Surveillance Society: Monitoring Everyday Life*, Buckingham, 2001.

⁵⁶ O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Oxford, 2022, F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (MA), 2015.

azionabili, ma per via di requisiti tecnici imposti a chi progetta sistemi e prodotti. Il GDPR ne è la matrice, con il principio di protezione dei dati fin dalla progettazione e per impostazione predefinita (art. 25) e con l'obbligo generale di sicurezza del trattamento (art. 32, che impone misure adeguate a garantire riservatezza, integrità, disponibilità e resilienza dei sistemi). Su questo asse si innestano due strumenti di portata più ampia: la Direttiva NIS2 (direttiva (UE) 2022/2555)⁵⁷, che eleva i requisiti di cibersecurity per le infrastrutture critiche e i servizi essenziali, estendendo l'ambito di applicazione a diciotto settori, e il Cyber Resilience Act (regolamento (UE) 2024/2847)⁵⁸, che trasferisce la responsabilità della sicurezza dal consumatore al fabbricante, imponendo requisiti obbligatori per tutti i prodotti con elementi digitali immessi sul mercato dell'Unione. Con coerenza logica la sicurezza è protetta non tanto attribuendo poteri agli utenti, quanto vincolando ex ante chi produce e gestisce le infrastrutture su cui gli utenti operano. È una scelta regolatoria che attribuisce al valore una densità giuridica peculiare, fatta di obblighi tecnici verificabili più che di posizioni soggettive azionabili.

Se, sul generale versante della vita privata, il GDPR costituisce l'asse portante della tutela, il diritto alla riservatezza delle comunicazioni elettroniche trova disciplina specifica nella Direttiva ePrivacy (direttiva 2002/58/CE)⁵⁹, che protegge la riservatezza delle comunicazioni e dei relativi metadati⁶⁰, vieta il tracciamento non autorizzato e subordina l'accesso alle informazioni archiviate sui dispositivi terminali degli utenti al consenso dell'interessato, fondamento giuridico che governa, tra l'altro, la disciplina dei cookie. La riforma di questo strumento è da anni bloccata in sede legislativa: la proposta della Commissione del 2017 prevedeva la sostituzione della direttiva con un regolamento direttamente applicabile, che

⁵⁷ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersecurity 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 NIS2).

⁵⁸ Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza).

⁵⁹ Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

⁶⁰ V. M. Orofino, *La tutela dei dati personali nelle comunicazioni elettroniche: dalla direttiva e-Privacy alla crisi del modello e-Privacy*, in G. De Minico – M. Orofino (a cura di), *Regole telecomunicazioni dati nell'Europa digitale*, Napoli, 2025, 31, F.J. Zuiderveen Borgesius - W. Steenbruggen, *The Right to Communications Confidentiality in Europe: Protecting Privacy, Freedom of Expression, and Trust*, in *Theoretical Inquiries in Law*, 19, 2019, 291.

avrebbe garantito uniformità applicativa e piena coerenza sistematica con il GDPR⁶¹. Tuttavia, il negoziato interistituzionale non ha ancora prodotto un testo definitivo. Sul piano delle fonti, la tutela della confidenzialità delle comunicazioni elettroniche che si fonda sulla Direttiva ePrivacy è oggi destinata a operare come *lex specialis* rispetto al GDPR, secondo una logica espressamente confermata dalla proposta di regolamento ePrivacy del 2017 (che ribadisce che tale disciplina «*particularise and complements*» il GDPR in materia di comunicazioni elettroniche). Si può osservare che la protezione della segretezza delle comunicazioni non tutela soltanto la sfera individuale della privacy, ma anche valori collettivi quali la libertà di espressione e, soprattutto, la *trust in communication services*, ossia la possibilità per individui e organizzazioni di affidare in sicurezza le proprie interazioni ai fornitori di servizi digitali. In questa prospettiva, la disciplina ePrivacy assume una funzione di rilievo costituzionale ulteriore rispetto al GDPR: non solo protezione del dato personale, ma presidio della fiducia infrastrutturale che rende possibile l'esercizio dei diritti della persona nello spazio comunicativo europeo.

Sul fronte dell'eredità digitale⁶², ossia il diritto di determinare cosa accada ai propri account e alle proprie informazioni dopo la morte, enunciato al punto 19 del Capitolo V, l'Unione non dispone ancora di uno strumento normativo armonizzato.

Per quanto concerne la protezione di bambini e giovani, l'AI Act vieta i sistemi di IA che sfruttano le vulnerabilità di una persona fisica dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il suo comportamento in modo da provocarle un danno significativo (art. 5, par. 1, lett. b)). Il DSA, come già visto, vieta alle piattaforme online di presentare inserzioni pubblicitarie basate sulla profilazione quando siano ragionevolmente consapevoli che il destinatario è minore (art. 28, par. 2) e impone loro di adottare misure adeguate e proporzionate per proteggere i minori, anche progettando le interfacce con il massimo livello di privacy e sicurezza per

⁶¹ La proposta (COM(2017) 10 final) è stata presentata dalla Commissione europea il 10 gennaio 2017, con il titolo "Proposta di Regolamento del Parlamento europeo e del Consiglio 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)". Sulla proposta v. F.J. Zuiderveen Borgesius - J. van Hoboken - R. Fahy - K. Irion - M. Rozendaal, *An assessment of the Commission's Proposal on Privacy and Electronic Communications*, Study for the LOBE Committee, 2017.

⁶² In argomento v. V. Confortini, *Persona e patrimonio nella successione digitale*, Torino, 2023, F. Bartolini - F.P. Patti, *Digital Inheritance and Post Mortem Data Protection: The Italian Reform*, in *European Review of Private Law*, 27(5), 2019, 118, E. Harbinja, *Does the Eu data protection regime protect post-mortem privacy and what could be the potential alternatives?*, in *Scripted*, 10, 1, aprile 2013.

impostazione predefinita (art. 28, par. 1, e considerando 71).

Come accennato, il corpus giurisprudenziale della Corte di giustizia in materia di sicurezza è il più ricco e consolidato tra tutti i capitoli della Dichiarazione. Il filone sulla riservatezza delle comunicazioni e il divieto di sorveglianza di massa si sviluppa da *Digital Rights Ireland* (C-293/12 e C-594/12 (2014)), in cui la Corte ha invalidato la Direttiva sulla conservazione dei dati, a *Tele2 Sverige e Watson* (C-203/15 e C-698/15 (2016)), dove i giudici hanno affermato che la conservazione generalizzata e indifferenziata dei dati di traffico è incompatibile con il diritto dell'Unione. *La Quadrature du Net* (C-511/18, C-512/18 e C-520/18 (2020)) ha segnato un passaggio ulteriore, estendendo l'applicabilità della direttiva 2002/58/CE alle misure nazionali adottate per finalità di sicurezza nazionale e respingendo in tal modo l'argomento degli Stati membri secondo cui tali misure esulerebbero dall'ambito del diritto dell'Unione. La Corte ha confermato il divieto di conservazione generalizzata e indifferenziata dei dati di traffico e localizzazione, ammettendo tuttavia che una minaccia grave, reale e attuale o prevedibile alla sicurezza nazionale possa giustificare un obbligo temporaneo di conservazione generale, purché sottoposto a controllo effettivo da parte di un giudice o di un'autorità amministrativa indipendente. La pronuncia ha inoltre fissato garanzie specifiche per l'analisi automatizzata dei dati, anticipando sul piano giurisprudenziale la logica di sorveglianza algoritmica controllata che il legislatore avrebbe successivamente codificato nell'AI Act. In *H.K. c. Prokuratuur* (C-746/18 (2021)) la Corte ha poi ribadito che l'accesso alle comunicazioni elettroniche da parte delle autorità pubbliche deve essere limitato, nel rispetto del principio di proporzionalità, alla lotta contro forme gravi di criminalità. Il filone sui trasferimenti internazionali dei dati è ben presidiato da *Schrems I* (C-362/14 (2015)) e *Schrems II* (C-311/18 (2020)), in cui la Corte di giustizia hanno rispettivamente invalidato il Safe Harbor e il Privacy Shield⁶³. Elaborata progressivamente lungo entrambi i filoni appare oramai consolidata la valutazione che una normativa che consenta alle autorità pubbliche di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche compromette l'essenza stessa del diritto garantito dall'art. 7 della Carta dei diritti fondamentali dell'Unione e costituisce oggi il riferimento costituzionale per la valutazione di qualsiasi regime di sorveglianza.

Il limite principale del Capitolo V rimane la tenuta dell'equilibrio tra sicurezza collettiva e libertà individuale. Le pressioni degli Stati membri per ampliare le capacità di accesso ai dati in nome della sicurezza pubblica

⁶³ In argomento, da ultimo, G. Proietti, *Tutela e valorizzazione dei dati nei mercati digitali. Il contratto, la concorrenza e i nuovi soggetti tutelati*, Milano, 2025, spec. cap. II, 89 e ss., A. Busacca, *Trasferimento dei dati personali UE-USA novità e criticità del data primacy framework*, in *federalismi.it*, 18 dicembre 2024.

(accentuate dal mutato contesto geopolitico successivo al febbraio 2022) continuano a mettere sotto tensione i confini tracciati dalla Corte di giustizia. Il caso più emblematico è il travagliato iter del regolamento sulla prevenzione degli abusi sessuali su minori online (noto come “Chat Control”⁶⁴). L’EDPB e l’EDPS hanno congiuntamente segnalato che l’obbligo generalizzato di scansione delle comunicazioni private avrebbe configurato una forma di sorveglianza di massa incompatibile con la giurisprudenza della Corte⁶⁵. Il Consiglio ha adottato nel novembre 2025 una posizione negoziale che eliminava l’obbligo generalizzato di scansione, mantenendo però un regime favorevole alla sorveglianza volontaria, sicché il trilogio è infine fallito nel marzo 2026 e il Parlamento europeo ha respinto anche la proroga del regime transitorio. Ne consegue che le piattaforme non possono più effettuare scansioni di massa dei messaggi privati, mentre i negoziati per un regolamento permanente restano aperti.

8. La sostenibilità ambientale e intergenerazionale

La sostenibilità ambientale e intergenerazionale resta il valore meno sviluppato e più programmatico dell’intera Dichiarazione del 2022: nessun altro capitolo presenta uno scarto altrettanto ampio tra l’ambizione valoriale proclamata e la densità giuridica degli strumenti che ne assicurano l’effettività. Il sesto capitolo della Dichiarazione (“Sostenibilità”) si articola in due enunciati fondamentali: i prodotti e i servizi digitali dovrebbero essere progettati, prodotti, utilizzati, riparati, riciclati e smaltiti in modo da attenuare il loro impatto negativo sull’ambiente. Vieppiù, ogni persona ha diritto ad accedere a informazioni precise sull’impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, «in modo da essere in grado di compiere scelte responsabili». Quest’ultimo enunciato incorpora implicitamente una dimensione intergenerazionale: il diritto all’informazione responsabile non tutela soltanto il consumatore presente, ma opera come argine contro il trasferimento sistematico dei costi ecologici della trasformazione digitale sulle generazioni future, alle quali verrebbero altrimenti consegnate le esternalità ambientali di scelte compiute oggi in condizioni di opacità informativa.

⁶⁴ Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce norme per la prevenzione e la lotta contro l’abuso sessuale su minori, COM(2022) 209 final, 11 maggio 2022. Sulla proposta di regolamento v. EPRS, *Proposal for a regulation laying down rules to prevent and combat child sexual abuse. Complementary impact assessment*, April 2023. In argomento v. R. Anderson, *Chat Control or Child Protection?*, 2022.

⁶⁵ EDPB e EDPS, *Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*, 28 luglio 2022.

La contraddizione strutturale tra transizione digitale e transizione verde non è all'evidenza risolvibile per via normativa in tempi brevi. La digitalizzazione dell'economia è stata presentata come leva della decarbonizzazione, ma richiede essa stessa infrastrutture ad alto consumo energetico (data center, reti 5G, sistemi di addestramento per l'intelligenza artificiale generativa) la cui impronta ambientale è in rapida crescita⁶⁶, in una maniera difficilmente compatibile con gli obiettivi climatici dell'Unione per come definiti dal regolamento (UE) 2021/1119⁶⁷. A questa tensione se ne sovrappone una seconda, di natura geopolitica: la sovranità digitale europea passa in misura crescente per la capacità computazionale autonoma, che richiede infrastrutture energivore localizzate nel territorio dell'Unione. Il perseguimento dell'autonomia strategica nel settore dell'IA e del cloud rischia così di entrare in conflitto diretto con gli impegni climatici, esponendo il modello europeo a una contraddizione interna che gli strumenti normativi adottati non hanno ancora affrontato in modo sistematico. Il Regolamento Ecodesign per Prodotti Sostenibili (regolamento (UE) 2024/1781⁶⁸) è lo strumento che più direttamente risponde agli impegni del Capitolo VI: estende i requisiti di progettazione ecocompatibile a quasi tutti i prodotti immessi sul mercato europeo e introduce il passaporto digitale di prodotto, uno strumento elettronico che rende accessibili le informazioni sulla sostenibilità ambientale del prodotto lungo l'intero ciclo di vita, inclusa la sua impronta di carbonio, le capacità di riparazione e le modalità di smaltimento. Il Data Act concorre su un piano diverso, in quanto il suo considerando 15 riconosce espressamente che i dati provenienti da prodotti connessi sono strumento per «tutelare l'ambiente, la salute e l'economia circolare, anche agevolando la manutenzione e la riparazione dei prodotti connessi», orientando in chiave ambientale la ratio dell'accesso ai dati disciplinato dal Capo II. L'AI Act affronta la dimensione energetica dell'intelligenza artificiale imponendo ai fornitori di modelli per finalità generali di includere nella documentazione tecnica «il consumo energetico noto o stimato del modello»⁶⁹, introducendo una misura di trasparenza che, per la prima volta, rende visibile su scala sistemica

⁶⁶ V. OECD, *Measuring the environmental impacts of artificial intelligence compute and applications*, OECD Digital economy papers, n. 341, November 2022.

⁶⁷ Regolamento (UE) 2021/1119 del Parlamento europeo e del Consiglio del 30 giugno 2021 che istituisce il quadro per il conseguimento della neutralità climatica e che modifica il regolamento (CE) n. 401/2009 e il regolamento (UE) 2018/1999 ("Normativa europea sul clima").

⁶⁸ Regolamento (UE) 2024/1781 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce il quadro per la definizione dei requisiti di progettazione ecocompatibile per prodotti sostenibili, modifica la direttiva (UE) 2020/1828 e il regolamento (UE) 2023/1542 e abroga la direttiva 2009/125/CE.

⁶⁹ Allegato XI, punto 2, lett. e), richiamato dall'art. 53, par. 1, lett. a).

l'impronta ambientale dei sistemi di IA. La Direttiva *Empowering Consumers for the Green Transition* (direttiva (UE) 2024/825⁷⁰) chiude il quadro introducendo nel regime delle pratiche commerciali sleali un divieto esplicito delle asserzioni ambientali ingannevoli: il collegamento con il Capitolo VI della Dichiarazione è diretto, poiché il diritto a informazioni precise sull'impatto ambientale dei prodotti digitali perde sostanza se le comunicazioni commerciali che veicolano tali informazioni possono essere costruite su affermazioni non verificate.

La Corte di giustizia non ha ancora sviluppato un corpus di pronunce specificamente dedicato alla sostenibilità dell'ecosistema digitale.

Il Capitolo VI della Dichiarazione è quello che misura con maggiore nitidezza la tenuta del modello europeo. Non si tratta di accertare la semplice coerenza tra valori proclamati e norme adottate, ma di verificare la compatibilità tra le ambizioni regolatorie sulla sostenibilità digitale e le scelte di governance tecnologica compiute in nome dell'autonomia strategica, che si muovono in direzioni opposte. La crescita dei consumi energetici legati all'IA generativa, al cloud computing e ai data center procede a ritmo nettamente superiore agli incrementi di efficienza prodotti dagli strumenti normativi vigenti. Colmare questo scarto è la condizione minima perché i valori del Capitolo VI non restino enunciazione programmatica.

9. Conclusioni: un antropocentrismo prevalentemente reattivo

Tutto quanto sopra illustrato, quale prima conclusione si può ragionevolmente ritenere che il modello europeo di regolazione dell'ecosistema digitale online abbia raggiunto una maturità sufficiente per essere valutato non più soltanto nei suoi strumenti, ma nella sua capacità di tradurre in obblighi concretamente esigibili e giurisdizionalmente effettivi i principi enunciati dalla Dichiarazione del 2022.

Tale valutazione risulta in un bilancio differenziato, poiché l'architettura regolatoria europea non ha tradotto con uguale intensità i valori della Dichiarazione del 2022.

La giurisdizionalizzazione procede in modo asimmetrico: è densa e consolidata per la sicurezza e la vita privata, mentre si assottiglia progressivamente per la libertà di scelta, la solidarietà e l'inclusione, la partecipazione al discorso pubblico, fino al limite estremo della sostenibilità ambientale,

⁷⁰ Direttiva (UE) 2024/825 del Parlamento europeo e del Consiglio, del 28 febbraio 2024, che modifica le direttive 2005/29/CE e 2011/83/UE per quanto riguarda la responsabilizzazione dei consumatori per la transizione verde mediante il miglioramento della tutela dalle pratiche sleali e dell'informazione.

per la quale la giurisprudenza della Corte è ancora del tutto embrionale. Questa asimmetria non è casuale, ma riflette la sequenza storica con cui i valori sono stati incorporati nel diritto dell'Unione. Il diritto alla vita privata e alla protezione dei dati aveva già trovato costituzionalizzazione negli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (su un fondamento normativo che affondava le radici nella direttiva 95/46/CE) quando la regolazione digitale online specifica ha cominciato a prendere forma come corpus autonomo. La sostenibilità ambientale dell'ecosistema digitale online, viceversa, è una categoria costruita *ex novo* dalla Dichiarazione del 2022, senza retroterra giurisprudenziale su cui fare leva. Il deficit più rilevante è tuttavia di ordine qualitativo. Il modello europeo appare aver privilegiato una declinazione prevalentemente difensiva dei valori proclamati, tutelando la persona dai rischi della tecnologia più di quanto la metta nelle condizioni di appropriarsi dei suoi benefici: un antropocentrismo reattivo più che promozionale, capace di proteggere, ma non ancora di emancipare. La Dichiarazione del 2022 parla di persone «nelle condizioni di perseguire le loro aspirazioni»: questa formulazione presuppone non solo l'assenza di ostacoli, ma la presenza attiva di risorse. Le competenze digitali, le interfacce accessibili, la distribuzione equa del potere informativo sono state garantite in modo disomogeneo, lasciando aperta la dimensione positiva dell'antropocentrismo: quella che non si esaurisce nella protezione, ma richiede abilitazione.

Un secondo piano di analisi riguarda il rapporto tra la Dichiarazione del 2022 e la giurisprudenza della Corte di giustizia. La logica dei valori della Dichiarazione del 2022 percorre sotterraneamente le pronunce della Corte, ma essa non compare come canone interpretativo esplicito in alcuna pronuncia: i suoi valori sono applicati senza essere nominati. Lo spazio tra il diritto proclamato e il diritto giurisdizionalizzato è ancora aperto, ed è su questo spazio che si misura la portata del costituzionalismo digitale europeo, inteso anzitutto come tentativo di estendere i vincoli valoriali del diritto costituzionale anche ai poteri privati che governano l'ecosistema digitale⁷¹. La Dichiarazione del 2022 si candida a divenire centrale documento assiologico del costituzionalismo digitale europeo, poiché ne esprime i valori fondativi, può orientare la produzione normativa e ne offre il parametro di coerenza interna. Il passaggio dalla candidatura alla piena operatività giuridica dipende da una condizione ancora non avverata: che la Corte di giustizia la incorpori come canone ermeneutico esplicito, com-

⁷¹ Sul costituzionalismo digitale europeo v. G. De Gregorio - O. Pollicino - P. Valcke (eds.), *The Oxford Handbook of Digital Constitutionalism*, Oxford, 2024; G. De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet: A Road towards Digital Constitutionalism?*, Oxford, 2021; E. Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, in *International Review of Law, Computer and Technology*, 33, 2019, 79.

piendo per la Dichiarazione del 2022 percorso analogo a quello che la giurisprudenza europea (ma anche nazionale) ha già compiuto per la Carta dei diritti fondamentali dell'Unione europea. Quel percorso ha una storia nota: in *Mangold* (C-144/04 (2005)) la Corte ha ricavato per la prima volta un principio generale (il divieto di discriminazione in ragione dell'età) dalle tradizioni costituzionali comuni e da strumenti di diritto derivato non ancora in vigore, affermandone l'efficacia orizzontale diretta in assenza di un esplicito fondamento nei Trattati. In *Kücükdeveci* (C-555/07 (2010)) quella costruzione è stata consolidata e ancorata esplicitamente all'art. 21 della Carta dei diritti fondamentali dell'Unione europea, convertendo un principio giurisprudenzialmente elaborato in diritto primario vincolante. È lo stesso meccanismo (dall'enunciazione valoriale all'operatività giuridica attraverso la mediazione giurisprudenziale) che *Google Spain* (C-131/12 (2014)) ha attivato nel dominio digitale per il diritto all'oblio: un diritto non scritto nei testi, ricavato per via interpretativa dalla Corte di giustizia e poi recepito dal legislatore nel GDPR. Il percorso è tracciato ed è stato già seguito con successo. La Dichiarazione del 2022 può ambire a farlo proprio.

A complicare il quadro interviene la pressione geopolitica. Il modello europeo è esposto a tensioni che provengono da due direzioni opposte: la spinta alla deregolazione in nome della competitività tecnologica e la tentazione, opposta, di rispondere alla dipendenza tecnologica con misure di controllo digitale che rischiano di erodere dall'interno i valori proclamati, di cui i dubbi e le incertezze sul regolamento Chat Control sono l'esempio più eloquente⁷².

La prima spinta trova nel Digital Omnibus l'espressione più rilevante e recente. Le due proposte gemelle presentate dalla Commissione il 19 novembre 2025 riaprono il cuore stesso dell'apparato regolatorio europeo a meno di tre anni dalla sua piena operatività, in nome della semplificazione e della competitività⁷³.

⁷² L. Carrer, *La strana alleanza tra big tech, Trump e l'estrema destra contro i diritti digitali in Europa*, in *Wired*, 5 febbraio 2026; A. Puliafito, *La retromarcia dell'AI Act si chiama digital omnibus*, in *Internazionale*, 3 dicembre 2025.

⁷³ Commissione UE, Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final, 19 novembre 2025; Proposal for a Regulation amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final, 19 novembre 2025. Per prime riflessioni v. G. González Fuster, *Caught Between AI and the AI Hype: How the Right to personal Data Protection was Ambushed*, in *Rivista di Diritti Comparati*, Spec. Issue VIII, 2026, 107; B. Carotti, *Contro il Digital Omnibus*, in *IRPA*, 18 novembre 2025;

Per quanto concerne la disciplina dei sistemi di intelligenza artificiale, si conferma la portata sistemica dell'intervento, poiché il testo di compromesso licenziato dal Coreper il 13 maggio 2026, in vista dell'adozione in prima lettura, ridefinisce alcuni snodi strutturali dell'AI Act⁷⁴. Sul piano dell'entrata in applicazione, le sezioni 1, 2 e 3 del Capo III, originariamente operative dal 2 agosto 2026, sono rinviate al 2 dicembre 2027 per i sistemi ad alto rischio dell'Allegato III e al 2 agosto 2028 per quelli dell'Allegato I, in ragione del ritardo nella predisposizione delle norme tecniche armonizzate e dell'assetto di governance nazionale. Sul piano sostanziale, viene introdotto un meccanismo orizzontale di limitazione degli obblighi del Capo III, Sezione 2, allorché la legislazione di armonizzazione settoriale elencata nella Sezione A dell'Allegato I garantisca un livello di protezione equivalente o superiore (nuovo art. 2, par. 13). L'elenco delle pratiche vietate viene esteso ai sistemi che generano o manipolano materiale intimo non consensuale e materiale di abuso sessuale su minori (nuovo art. 5, par. 1, lett. ba e bb), in una direzione che rafforza, anziché ridurre, la protezione di posizioni soggettive fondamentali. Specularmente, però, l'obbligo di alfabetizzazione dei fornitori e dei deployers (art. 4) è ricondotto da obbligo di risultato a obbligo di mezzi, e la competenza esclusiva dell'AI Office è ampliata ai sistemi costruiti su modelli per finalità generali sviluppati dalla medesima impresa e a quelli integrati in piattaforme e motori di ricerca *very large* ai sensi del DSA, con un articolato apparato di poteri ispettivi e sanzionatori (nuovi artt. 75-75e). L'insieme di queste modifiche, intervenendo simultaneamente sul perimetro applicativo, sulla tassonomia delle pratiche vietate, sull'architettura di vigilanza e sul cronoprogramma dell'entrata in vigore, appaiono eccedere la categoria della mera semplificazione e configurare piuttosto una rivisitazione di non poco momento. La proposta sulla disciplina dei dati, viceversa, resta in negoziato e divide i co-legislatori in particolare sulla ridefinizione soggettiva e relativa della nozione di dato personale, su cui EDPB ed EDPS hanno espresso nel febbraio del 2026 un parere congiunto problematico⁷⁵. È sottolineato come la riforma trascenda la dichiarata finalità di codificazione della giurisprudenza della Corte di giustizia (di cui isola selettivamente un solo elemento,

E. Tripodi - G. Cassano, *Il «Digital Omnibus»: semplificazione (o deregolamentazione) del contesto digitale europeo?*, in *Rivista dell'Internet*, 1, 2026.

⁷⁴ L'orientamento generale del Consiglio del 13 marzo 2026 (doc. 7322/26) e la posizione del Parlamento europeo adottata il 26 marzo 2026, hanno condotto all'accordo provvisorio del 6 maggio 2026, confermato dal Coreper il 13 maggio 2026 (doc. 9247/26).

⁷⁵ V. EDPB-EDPS, *Joint Opinion 02/2026 on the proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, 10 febbraio 2026, in *edpb.europa.eu*.

dilatandolo oltre il perimetro tracciato in *EDPS c. SRB*⁷⁶) e introduca una definizione costruita per via negativa, generatrice di incertezza applicativa. Viene ritenuto che essa restringa in modo strutturale l'ambito materiale del GDPR, con effetti diretti sul livello di protezione dei dati personali quale diritto fondamentale ex art. 8 della Carta dei diritti fondamentali. Criticata è anche la delega alla Commissione, per via di atto di esecuzione, scelte che attengono ai confini stessi della tutela.

Letto attraverso la lente dell'antropocentrismo reattivo, il Digital Omnibus è qualcosa di più di un intervento di manutenzione. È il test che misura la stabilità stessa del modello regolatorio europeo. Se la costituzionalizzazione difensiva consolidata nel decennio scorso fosse stata radicata in un baricentro valoriale stabilizzato, una riapertura di tale ampiezza, a tale distanza dall'entrata in vigore degli atti modificati, non sarebbe stata politicamente concepibile. La rapidità con cui le difese costruite intorno alla persona possono essere rinegoziate, quando lo richiede l'argomento della competitività, conferma che l'antropocentrismo europeo non ha ancora trovato l'ancoraggio strutturale che la Dichiarazione del 2022 prometteva. Ne resta, per ora, la dimensione reattiva, esposta come ogni postura difensiva alla pressione delle congiunture.

Le due spinte, deregolatoria e securitaria, convergono in un unico effetto: restringere lo spazio entro cui il modello europeo può sviluppare la sua vocazione promozionale, riducendolo a una funzione difensiva che esso ha già dimostrato di saper esercitare, ma che non esaurisce l'ambizione valoriale della Dichiarazione del 2022.

Colmare il divario fra un diritto della protezione e un diritto dell'emancipazione digitale, passare dalla tutela reattiva all'abilitazione positiva dell'autonomia individuale e collettiva nell'ambiente digitale, è la sfida che la prossima stagione regolatoria dell'Unione ha davanti per dare completezza al modello valoriale europeo. Non si tratta di abbandonare la logica della protezione, ma di arricchirla: costruire le condizioni materiali (competenze, infrastrutture, distribuzione del potere informativo) senza le quali i diritti proclamati restano asimmetrici rispetto alle dinamiche di potere che governano l'ecosistema digitale online. È in questo passaggio dalla protezione alla emancipazione ed *empowerment* che si gioca la maturazione del costituzionalismo digitale europeo: non più soltanto limite al potere tecnologico, ma costruzione giuridica delle condizioni materiali dell'autonomia informazionale della persona nello spazio digitale dell'Unione. Dare a questo statuto digitale europeo della persona una forma giuridica compiuta, definirne il contenuto, i titolari, le condizioni di esercizio e i meccanismi di tutela, è il compito teorico che la stagione regolatoria descritta lascia aperto.

⁷⁶ CGUEC-413/23 P, *EDPS c. SRB* (2025).

Abstract

Viene analizzato il modello europeo di regolazione dell'ecosistema digitale europeo online attraverso la lente assiologica della Dichiarazione europea sui diritti e i principi digitali del 2022, assunta come cornice valoriale dell'intero corpus normativo dell'Unione. Il metodo adottato assume i valori proclamati dalla Dichiarazione del 2022 come categorie ordinanti per testare la coerenza materiale del diritto derivato: oggetto dell'analisi è la capacità degli atti normativi adottati nell'ultimo decennio dalle istituzioni europee di tradurre i principi in obblighi giuridicamente esigibili e standard giurisprudenziali effettivi. La tesi centrale è che il modello europeo abbia sviluppato una costituzionalizzazione prevalentemente difensiva dell'ecosistema digitale: più efficace nel limitare i rischi tecnologici che nel costruire condizioni positive di autonomia informazionale. Questa postura viene definita "antropocentrismo reattivo", capace di proteggere, ma non ancora di emancipare l'individuo dai bisogni digitali. Il saggio esamina in successione i sei valori della Dichiarazione del 2022 (centralità della persona, solidarietà e inclusione, libertà di scelta, partecipazione democratica, sicurezza e protezione, sostenibilità ambientale e intergenerazionale), misurando per ciascuno lo scarto tra proclamazione e giurisdizionalizzazione. Il bilancio complessivo individua nel passaggio dalla tutela reattiva all'abilitazione positiva dell'autonomia individuale e collettiva la sfida aperta della prossima stagione regolatoria europea.

This article analyses the European model for regulating the online digital ecosystem through the axiological lens of the 2022 European Declaration on Digital Rights and Principles, taken as the value framework of the Union's entire normative corpus. The methodology treats the values proclaimed by the 2022 Declaration as organising categories against which to test the substantive coherence of secondary law: the inquiry focuses on the capacity of the legislative acts adopted over the past decade by the European institutions to translate principles into legally enforceable obligations and effective judicial standards. The central thesis is that the European model has developed a predominantly defensive constitutionalisation of the digital ecosystem, more effective in containing technological risks than in constructing positive conditions for informational autonomy. This posture is defined as "reactive anthropocentrism": capable of protecting, but not yet of emancipating, the individual from digital dependencies. The article examines in turn the six values of the 2022 Declaration (centrality of the person, solidarity and inclusion, freedom of choice, democratic participation, safety and protection, environmental and intergenerational sustainability), measuring for each the gap between proclamation and justiciability. The overall assessment identifies the transition from reactive

Raffaele Torino

protection to the positive enablement of individual and collective autonomy as the open challenge of the next European regulatory season.

Keywords

European digital ecosystem – European values – digital rights – digital constitutionalism – 2022 European Declaration on Digital Rights and Principles