I valori fondamentali dell'Unione europea nell'ecosistema digitale

Raffaele Torino

Il presente numero monografico raccoglie (e di questo ringrazio la *Rivista di diritto dei media* e gli amici Oreste Pollicino e Marco Bassini) undici contributi selezionati nell'ambito della *call for papers* 2024-2025 promossa dalla Cattedra Jean Monnet "*EU Values in the Online Digital Environment*" dell'Università degli Studi Roma Tre di cui sono titolare.

Il problema comune che attraversa i contributi è se, e a quali condizioni, i valori fondamentali dell'Unione riescano ancora a operare come criteri effettivi di orientamento giuridico in un ecosistema digitale governato da infrastrutture private, processi automatizzati e forme di potere difficilmente riconducibili alle categorie tradizionali del mercato.

I contributi si misurano con questa domanda da angolature disciplinari diverse (diritto dell'Unione europea, diritto privato comparato, diritto costituzionale, diritto amministrativo, diritto della concorrenza, economia) e su oggetti normativi distinti: dal Regolamento sui servizi digitali (DSA) al Regolamento sui mercati digitali (DMA), dall'AI Act al Regolamento sulla pubblicità politica, passando per il GDPR e le prospettive *de lege ferenda* legate alla crittografia post-quantistica. Ne emerge una mappa delle tensioni più acute che attraversano oggi la regolazione dell'ecosistema digitale europeo, organizzata attorno a tre assi tematici.

Il primo asse riguarda la natura e le implicazioni giuridiche del potere esercitato dalle grandi piattaforme digitali, un potere che eccede la nozione tradizionale di posizione dominante e che la dottrina ha cominciato a denominare con espressioni come *Digital Power* o *Modern Bigness*.

Elisabeth Wondracek affronta questa questione in termini sistematici e propone una rilettura dell'intero quadro regolatorio europeo alla luce della necessità di imporre obblighi costituzionali diretti agli attori digitali privati che esercitano un potere di fatto regolatorio[1]. La sua analisi muove dalla constatazione che gli strumenti esistenti (l'art. 102 TFUE, il DMA e il DSA) sono concepiti per rispondere a forme di potere essenzialmente economiche, misurabili in termini di quote di mercato o effetti sui prezzi, e che risultano pertanto strutturalmente inadeguati a captare le manife-

[1] E. Wondracek, *Balancing Power and Responsibility in Digital Markets – The Direct Horizontal Enforcement of the EU Values.*

stazioni più profonde del potere digitale: il controllo del discorso pubblico attraverso algoritmi opachi, la manipolazione delle preferenze tramite tecniche di *hypernudging*, l'esercizio di funzioni quasi-giudiziarie attraverso la moderazione dei contenuti. La proposta avanzata (l'applicazione orizzontale diretta della Carta dei diritti fondamentali nei confronti di soggetti privati che detengono potere regolatorio di fatto) si inserisce in un dibattito dottrinale ormai maturo, che il contributo arricchisce con una ricognizione critica della giurisprudenza della Corte di giustizia in materia di effetti orizzontali sia delle libertà fondamentali sia dei diritti della Carta.
Sul versante istituzionale, Federica Pagnotta porta al centro un nodo difficilmente eludibile: come conferire all'esecutivo europeo margini di manovra sufficientemente ampi da inseguire la velocità del progresso tecnologico senza sottrarre al circuito rappresentativo decisioni che incidono su aspetti essenziali della tutela dei diritti fondamentali[2]. La riflessione si estende alla giurisprudenza più recente del Tribunale dell'Unione europea (in particolare le sentenze *Blindl* e *Latombe*) che, nell'avviso dell'Autrice, segnalano un preoccupante cambiamento di orientamento rispetto all'approccio garantista consolidato dalla Corte di giustizia nelle sentenze *Schrems I* e *Schrems II*, con il rischio concreto di indebolire la protezione dei dati personali dei cittadini europei nei trasferimenti verso gli Stati Uniti.
Una diversa angolatura sul medesimo problema è quella di Vincenzo Forte e Alessio Scaffidi, che ricostruiscono la portata dell'art. 25 DSA (il quale introduce un divieto assoluto di *dark patterns*) seguendo il percorso evolutivo che dalla Direttiva e-Commerce conduce al DSA[3]. Al suo centro c'è un passaggio che vale la pena segnalare: il diritto digitale europeo non disciplina più soltanto la veridicità del messaggio commerciale, ma la struttura stessa dell'interfaccia, concepita come condizione architettonica della libertà cognitiva dell'utente. La tesi (che il rinvio alla Direttiva sulle pratiche commerciali sleali (UCPD) operato dall'art. 25, par. 2, DSA debba essere letto come clausola di coordinamento negativo e non come subordinazione ermeneutica) ha conseguenze concrete: trattare il divieto di *dark patterns* come parametro interpretativo della UCPD significherebbe privarlo della sua autonomia precettiva, riducendo a *soft law* una norma di rango regolamentare.
La prospettiva si allarga con il contributo di Anna Vicinanza[4], che esamina in modo integrato le disposizioni del DSA, del DMA e del Regolamento

[2] F. Pagnotta, *Il ruolo della Commissione nella governance del mercato unico digitale tra competenze e rispetto dei valori.*

[3] V. Forte – A. Scaffidi, *Tra innovazione normativa e frammentazione giuridica: il caso dei* dark patterns *nell'Unione europea digitale.*

[4] A. Vicinanza, *User Autonomy and Algorithmic Recommendations under the Digital Services Act, the Digital Markets Act, and the Political Advertising Regulation.*

sulla pubblicità politica relative ai sistemi di raccomandazione algoritmici, verificandone l'attuazione concreta attraverso un'osservazione empirica del comportamento di Meta e TikTok. Ne emerge un quadro a due velocità: i progressi sono reali (in particolare il divieto di profilazione basata su categorie particolari di dati e l'obbligo di offrire un'alternativa non profilata) ma convivono con limiti persistenti, dalla vaghezza delle descrizioni fornite agli utenti sulle logiche di raccomandazione alla tendenza delle piattaforme a interpretare in senso minimalista gli obblighi di trasparenza. Di particolare interesse è l'analisi del modello «pay or consent» di Meta, al centro di un procedimento della Commissione europea conclusosi con una sanzione significativa, e la questione ancora aperta della sua compatibilità con il DMA.

Il secondo asse tematico ha al suo centro la qualità del discorso pubblico e le condizioni strutturali della deliberazione democratica nell'era algoritmica. I contributi di Sara Gallone e Giulia Napoli affrontano questa questione partendo da premesse teoriche distinte, ma approdano a una diagnosi comune: la disinformazione è una minaccia che gli strumenti meramente repressivi non bastano a contenere senza rischiare derive censorie incompatibili con la libertà di espressione.

Sara Gallone muove da una ricostruzione teorica della libertà di espressione nella tradizione liberal-democratica, distinguendo la dimensione attiva (libertà di informare) da quella passiva (diritto a essere informati), per poi esaminare due casi giurisprudenziali di sicuro rilievo[5]. La sentenza del Tribunale dell'Unione europea nel caso *RT France c. Consiglio* e la decisione della Corte costituzionale rumena che, nel dicembre 2024, ha annullato le elezioni presidenziali in ragione di una campagna di disinformazione coordinata condotta attraverso TikTok con finanziamenti riconducibili a sfere di influenza russa, offrono due esempi paradigmatici della funzione democratica della libertà di espressione come diritto pubblico che può giustificare misure di contrasto alla disinformazione quando essa minacci la sicurezza, l'ordine pubblico o il corretto funzionamento del processo elettorale. La parte normativa del contributo esamina il DSA e il regolamento (UE) 2024/900 come strumenti di una regolazione procedurale che, operando sui flussi informativi più che sui contenuti, mira a garantire un livello minimo di qualità del dibattito pubblico compatibile con il pluralismo.

Su un piano diverso si muove Giulia Napoli[6], che concentra l'attenzione sulla dimensione più delicata del diritto all'informazione: l'Autrice argomenta che esso non può tradursi in un diritto soggettivo alla «corretta»

[5] S. Gallone, *Diritto all'informazione e dibattito pubblico nell'era della disinformazione: una prospettiva europea tra giurisprudenza e strumenti normativi.*

[6] G. Napoli, *Tutela dei processi democratici e diritto all'informazione: la risposta europea di contrasto alla disinformazione nella società algoritmica.*

informazione senza scivolare verso un insostenibile monopolio della verità, e che il rischio è oggi amplificato dai sistemi di intelligenza artificiale generativa. La costruzione del consenso nell'era dell'IA (in cui modelli generativi e moderativi si combinano per saturare il discorso pubblico di contenuti sintetici ottimizzati per massimizzare l'*engagement*) non è una versione aggiornata della disinformazione tradizionale: è una minaccia qualitativamente diversa alla dialettica democratica. Il punto più originale del contributo è la proposta finale: quella stessa tecnologia potrebbe essere riorientata, se progettata secondo il principio del *diversity by design*, verso il contrasto delle bolle informative e la promozione di un'esposizione plurale. Chi decide i criteri del pluralismo rimane una domanda aperta, ma il contributo indica con precisione le condizioni strutturali entro cui porla.

Il terzo asse raccoglie i contributi che affrontano l'intelligenza artificiale come oggetto specifico di regolazione, esaminando le tensioni interne all'AI Act e le sue interazioni con il diritto privato, il diritto amministrativo e le sue implicazioni sul diritto della crittografia e della sicurezza informatica.

Il nodo del "diritto alla spiegazione" introdotto dall'art. 86 dell'AI Act è al centro del contributo di Julian Colamedici[7], il quale lo colloca nel quadro della giurisprudenza del Consiglio di Stato italiano. Sin dalla sentenza n. 8472 del 2019, quell'orientamento ha elaborato i principi di conoscibilità, non esclusività algoritmica e non discriminazione algoritmica come requisiti minimi per l'uso dell'IA nell'attività provvedimentale; con la sentenza n. 4929 del 2025 ha poi qualificato i sistemi di IA come «modulo procedimentale» volto a svolgere l'attività autoritativa in modalità più efficienti. Il confronto tra l'art. 86 dell'AI Act e l'art. 22 del GDPR (sviluppato attraverso la formula, mutuata da Kaminski e Malgieri, del diritto alla spiegazione come norma al tempo stesso «più forte e più debole» rispetto alla disciplina previgente) consente di cogliere un progresso reale nell'estensione del diritto alle decisioni semi-automatizzate, e insieme una lacuna: l'assenza di meccanismi di tutela analoghi a quelli previsti dall'art. 22, par. 3, GDPR, che la legge italiana n. 132/2025 contribuisce in parte a colmare.

Federico D'Orazio affronta una questione per certi versi speculare: non il diritto dell'individuo a contestare la decisione algoritmica, ma la struttura contrattuale che rende possibile o impossibile l'esercizio di quel diritto[8]. Il suo contributo analizza i contratti di fornitura dei sistemi di IA tra *provider* e *deployer* come livello regolatorio che opera nell'ombra della legislazione su IA e protezione dei dati, potenzialmente svuotandone l'effettività. La sentenza della Corte di giustizia nel caso *Schufa* è utilizzata come punto

[7] J. Colamedici, *Intelligenza artificiale e processi decisionali pubblici alla luce dell'AI Act: il "diritto alla spiegazione" ex art. 86 del Regolamento.*

[8] F. D'Orazio, *The Contractual Governance of AI between the Public and Private Sectors: Transparency and Explainability as Contractual Obligations?*

di partenza per una riflessione più generale sulla natura regolatoria dei contratti di approvvigionamento dell'IA. La tesi che l'art. 13 dell'AI Act operi come fonte di regolazione contrattuale (trasformando il dovere del *provider* di trasmettere le informazioni necessarie per interpretare e spiegare gli *output* del sistema in un obbligo contrattuale la cui violazione integra inadempimento) è sorretta da una ricognizione comparatistica che include la dottrina tedesca del *Vertrag mit Schutzwirkung für Dritte*, proposta come strumento per fondare la legittimazione delle persone lese a richiedere il risarcimento del danno direttamente contro il fornitore.

Il problema della qualità dei dati emerge con particolare nettezza nel contributo di Tamar Navdarashvili[9], che sposta l'attenzione dalla sola architettura del modello alla fase, spesso meno visibile ma decisiva, della costruzione del dataset. La tesi è che la riduzione delle discriminazioni algoritmiche non possa essere perseguita soltanto intervenendo sull'*output* del sistema, ma debba risalire alla genealogia tecnica e documentale del dato: la qualità, la rappresentatività, la trasparenza. Particolare attenzione è dedicata ai dati sintetici, strumento promettente per ridurre la dipendenza da dati sensibili reali, ma capace di replicare, con una patina di neutralità, i *bias* dei dati originali; di qui la proposta di estendere loro le stesse esigenze di documentazione strutturata ispirate al modello delle *datasheets for datasets* di Gebru et al., che l'AI Act già impone per i dati reali. Quel che il contributo mostra con chiarezza è che il problema del *bias* non può essere trattato come una questione di soli output discriminatori: è, prima ancora, una questione di dati.

Il rapporto tra regolazione e innovazione assume una dimensione istituzionale ed economica nel contributo di Filippo Bagni e Luciana Lazzeretti[10], i quali collocano le *regulatory sandboxes* introdotte dall'AI Act all'interno della più ampia architettura degli strumenti europei di supporto all'innovazione: dai Centri europei di innovazione digitale (EDIH) alle Testing and Experimentation Facilities (TEF), fino alle AI Factories. La loro tesi è che le *sandbox* non vadano lette come mere deroghe temporanee al quadro normativo, ma come infrastrutture di apprendimento reciproco tra regolatori e imprese, capaci di produrre conoscenza tecnico-regolatoria che alimenta la formazione di standard futuri. L'analisi del regolamento di attuazione dell'AI Act, nella versione di dicembre 2024, fa emergere tanto le potenzialità del modello quanto i rischi (frammentazione interistituzionale, *forum shopping* tra Stati membri, cattura regolatoria) che ne possono limitare l'efficacia.

In chiusura, il contributo di Davide Clementi introduce una prospettiva

[9] T. Navdarashvili, *From Raw to Right: When Data Becomes Good for Bias Mitigation.*

[10] F. Bagni – L. Lazzeretti, *Regulation Meets Innovation in AI: The Role of Regulatory Sandboxes in the EU Digital Ecosystem.*

che guarda oltre il presente regolatorio e pone una questione destinata a diventare sempre più urgente: la preparazione dell'Unione europea all'avvento del calcolo quantistico come obbligo costituzionale fondato sull'art. 2 TUE e sul dovere di preservare l'effettività dei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta dei diritti fondamentali[11]. L'argomento procede per gradi: i computer quantistici renderanno obsoleti gli attuali schemi crittografici a chiave pubblica (RSA e crittografia a curve ellittiche) esponendo alla decrittazione retroattiva («harvest now, decrypt later») archivi di dati medici, corrispondenza diplomatica, registri di proprietà intellettuale e qualsiasi informazione oggi protetta da questi algoritmi. La conseguenza giuridica, sviluppata attraverso la giurisprudenza della Corte di giustizia da *Digital Rights Ireland* a *Schrems II*, è l'emergere di un obbligo positivo di previsione tecnologica: non agire equivarrebbe a una omissione strutturale nella tutela dei diritti fondamentali. Le proposte istituzionali avanzate (un Codice digitale europeo e un Quantum Secure Data Protocol (QSDP) come cornice modulare di requisiti crittografici minimi) sono ambiziose, e la loro valutazione critica è esplicitamente parte dell'argomentazione.

Dalla lettura complessiva ritengo che non emerga una risposta rassicurante. Il quadro normativo europeo è ricco, sofisticato, talvolta persino anticipatorio, ma non ancora pienamente stabilizzato rispetto alle trasformazioni che pretende di governare. Proprio per questo, i contributi non si limitano a registrare insufficienze: ciascuno individua un punto di attrito (istituzionale, contrattuale, tecnologico o assiologico) dal quale può prendere forma una diversa traiettoria di sviluppo della regolazione dell'ecosistema digitale europeo.

Da qui deriva, a mio avviso, l'interesse principale del complesso dei contributi: non offrire una teoria unitaria del diritto digitale dell'Unione europea, ma mostrare come la tenuta dei valori dell'Unione dipenda ormai da snodi regolatori molto concreti: architetture delle piattaforme, contratti di fornitura dell'IA, qualità dei dati, poteri delegati della Commissione, infrastrutture crittografiche. È su questi snodi che si misurerà, nei prossimi anni, la capacità del diritto europeo di trasformare i valori dell'Unione in criteri effettivi di governo dell'ecosistema digitale.

La riflessione avviata con questo numero è destinata a proseguire. La *call for papers* 2025-2026 è già in corso, e nuove ricerche e riflessioni si aggiungeranno a quelle raccolte in questo numero della rivista.

Mi piace, infine, rivolgere un ringraziamento personale ai membri del Comitato scientifico della Cattedra Jean Monnet "*EU Values in the Online Digital Environment*" (Marco Bassini, Marina Castellaneta, Elisa Giomi, Antonio Iannuzzi, Jacques Moscianese, Oreste Pollicino e Marco Scialdone)

[11] D. Clementi, *Quantum Preparedness as a Constitutional Obligation for the European Union.*

per aver contribuito con competenza e generosità alla selezione e alla valutazione dei lavori.
Un ringraziamento del tutto speciale va a Leda Colamartino, collaboratrice della Cattedra, senza il cui instancabile impegno questo numero monografico non avrebbe visto la luce.