

Digital Data Sovereignty: diritto e democrazia nell'età algoritmica

Elisa Sorrentino*

DIGITAL DATA SOVEREIGNTY: LAW AND DEMOCRACY IN THE ALGORITHMIC AGE

ABSTRACT: This contribution addresses the crisis of democratic legitimacy induced by algorithmic governance, proposing a reconceptualisation of digital data sovereignty as an emerging form of infrastructural power exceeding data protection paradigms. Through three converging axes, namely sovereignty as a protective office serving the citizen, datafication as a structural reorganisation of the informational environment, and the application of FAIR principles as FAIR by design, the paper develops a conceptual architecture seeking to align technological innovation with democratic imperatives. The HAIMLA methodology is proposed as a procedural device for intelligibility and accountability of automated decisions, framing digital constitutionalism as a systemic response to the asymmetries of informational power.

KEYWORDS: digital sovereignty; algorithmic governance; FAIR principles; digital constitutionalism; HAIMLA

ABSTRACT: Il contributo affronta la crisi di legittimità democratica indotta dalla governance algoritmica, proponendo una riconcettualizzazione della *digital data sovereignty* come forma emergente di potere infrastrutturale che eccede i paradigmi della *data protection*. Attraverso tre assi convergenti, ossia la sovranità come *protective office* al servizio del cittadino, la *datafication* come riorganizzazione strutturale dell'ambiente informativo e l'applicazione dei principi FAIR declinati come FAIR *by design*, lo scritto elabora un'architettura concettuale finalizzata a orientare l'innovazione tecnologica entro imperativi democratici. La metodologia HAIMLA viene proposta quale dispositivo procedurale di intelligibilità e responsabilità delle decisioni automatizzate, configurando il costituzionalismo digitale come risposta sistemica alle asimmetrie del potere informazionale.

PAROLE CHIAVE: sovranità digitale; governance algoritmica; principi FAIR; costituzionalismo digitale; HAIMLA

SOMMARIO: 1. Introduzione – 2. La sovranità informazionale oltre la *data protection* – 3. Dal dato al potere. Opacità algoritmica, sovranità informazionale e *governance* costituzionalmente orientata – 4. I principi FAIR come presidio

* CTER, presso Istituto di Informatica e Telematica del CNR, Sede di Cosenza. Mail: elisa.sorrentino@iit.cnr.it. Contributo sottoposto a doppio referaggio anonimo.

costituzionale della *governance* algoritmica – 5. Costituzionalismo digitale e i confini del paradigma regolatorio tradizionale – 6. Conclusioni.

1. Introduzione

La crisi di legittimità democratica indotta dalla *governance* algoritmica¹, nelle sue forme più opache e asimmetriche², sfugge a rimedi circoscritti alla tutela della privacy individuale o a strumenti regolatori meramente procedurali. Essa esige, piuttosto, un riposizionamento teorico radicale della sovranità³, in cui la *digital data sovereignty*⁴ si configura come forma emergente di potere costitutivo e normativo, capace di riconfigurare il nesso tra episteme, ius e demos nell'ecosistema digitale. L'argomentazione si articola lungo tre assi convergenti, che sono il fondamento teorico della sovranità come *protective office* al servizio del cittadino⁵; la dimensione epistemica della *datafication*⁶ quale riorganizzazione strutturale dell'ambiente informativo; e la proposta di fondare il costituzionalismo digitale sui principi FAIR⁷ declinati come *FAIR by design*⁸, affiancati dalla metodologia HAIMLA quale dispositivo procedurale di intelligibilità e responsabilità democratica delle decisioni automatizzate. Il fondamento teorico di questa prospettiva è offerto dalla *pars construens* di Anne Peters⁹, che ridefinisce la sovranità non più come Letztbegründung assoluta del diritto internazionale, ma come *protective office* ontologicamente subordinato all'umanità, principio normativo supremo che impone il rispetto e la promozione dei diritti, degli interessi, dei bisogni e della sicurezza delle persone. In tale quadro, i conflitti tra sovranità statale e diritti fondamentali non si risolvono mediante un bilanciamento tra posizioni equiordinate, ma devono essere orientati da una presunzione a favore dell'umanità quale criterio assiologico prioritario. Ne deriva una riconfigurazione della sovranità come *munus* protettivo, con i relativi obblighi giuridici di protezione e le forme strutturali di *accountability* regolativa¹⁰, in cui il rapporto tra Stato e cittadino si trasforma da rapporto di dominio a relazione fiduciaria, nella quale il potere pubblico opera quale agente responsabile nei confronti di un principale collettivo, titolare di diritti cognitivi e informativi. Su questo sfondo teorico, l'umanizzazione della sovranità assume contorni drammaticamente concreti alla luce del «surveil-

¹Per una mappatura sistematica del dibattito sulla *governance* algoritmica si vedano: R. DIAKOPOULOS, *Algorithmic accountability: Journalistic investigation of computational power structures*, in *Digital Journalism*, 3(3), 2015, 398-415.

²F. MUSIANI, *Governance algoritmica: sorveglianza, censura e diritti fondamentali*, in F. FOSSA, V. SCHIAFFONATI, G. TAMBURRINI (a cura di), *Automi e persone. Introduzione all'etica dell'intelligenza artificiale e della robotica*, Brescia 2021, 95-113.

³R. BIN, *La sovranità nazionale e la sua erosione*, in A. PUGIOTTO (a cura di), *Per una consapevole cultura costituzionale. Lezioni magistrali*, Napoli 2013, 369-381.

⁴G. FINOCCHIARO, *Data and Digital Sovereignty*, in *European Review of Digital Administration & Law*, 3(2), 2023, 9-12.

⁵A. PETERS, *Humanity as the A and Ω of Sovereignty*, in *European Journal of International Law*, 20(3), 2009, 51-544.

⁶U.A. MEJIAS, N. COULDRY, *Datafication*, in *Internet Policy Review*, 8(4), 2019. Il termine designa la quantificazione dell'esperienza umana attraverso l'informazione digitale, spesso a fini economici, con conseguenze sociali sull'intersezione tra potere e conoscenza.

⁷M.D. WILKINSON et al., *The FAIR guiding principles for scientific data management and stewardship*, in *Scientific Data*, 3(1), 2016, 1-9; Go FAIR Initiative, <https://www.go-fair.org/fair-principles/> (last visited 23/06/2026).

⁸E. SORRENTINO, A.F. SPAGNUOLO, *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto*, 6(2), 2024, 685-701.

⁹A. PETERS, *op. cit.*

¹⁰A. DOSHI-VELEZ et al., *Accountability of AI under the law: The role of explanation*, 2017.



lance capitalism» teorizzato da Shoshana Zuboff, un nuovo *nomos* istituzionale fondato sulla mercificazione predatoria del comportamento umano e sull'asimmetrica concentrazione di conoscenza computazionale¹¹. Tale regime opera mediante un'ubiqua «architettura di riferimento», il «Big Other», che non si limita a sorvegliare, ma interpone un livello intermedio tra soggetto e mondo, estraendo surrettiziamente dati comportamentali per prevedere e modificare *ex ante* le condotte individuali, riducendo l'umano a *dividuo* ed erodendo le fondamenta dell'autodeterminazione e dell'ordine democratico¹². La sovranità digitale¹³ si configura così come antidoto imperativo contro l'espansione transnazionale del potere corporativo, che minaccia di privatizzare il governo cognitivo-normativo un tempo appannaggio statale. Proprio per questo, il dibattito corrente sulla *digital data sovereignty*¹⁴ e sulla *governance algoritmica*, incentrato prevalentemente sulla salvaguardia dei dati personali¹⁵, non dovrebbe risolversi né in una mera proiezione della sovranità statale, né in una questione di conformità normativa ma esige un radicale *concept reengineering*¹⁶. Di fronte a tali sfide, il GDPR¹⁷ attenua l'estrazione predatoria di dati comportamentali, ma si rivela strutturalmente inadeguato a fronteggiare una governance algoritmica opaca e sorvegliante¹⁸. Diviene pertanto imprescindibile elaborare meccanismi robusti di *accountability*, trasparenza ed esplicabilità, unitamente a forme effettive di controllo pubblico, al fine di elevare l'autonomia digitale a presupposto sostanziale di legittimità democratica.

2. La sovranità informazionale oltre la *data protection*

La crescente centralità del dato digitale segnala l'emersione di una forma di potere infrastrutturale che non coincide più con la mera traccia soggettiva, ma incide in modo strutturale sulla configurazione della

¹¹S. ZUBOFF, *The Age of Surveillance Capitalism*, in *Social Theory Re-Wired*, New York-London, 2023, 203-213.

¹²S. ZUBOFF, *Big other: Surveillance capitalism and the prospects of an information civilization*, in *Journal of Information Technology*, 30(1), 2015 75-89. Cfr. sul concetto lacaniano del "Big Other" S. ŽIŽEK, *The Puppet and the Dwarf. The Perverse Core of Christianity*, Cambridge (MA), 2003; e il concetto di "dividuo" in G. DELEUZE, *Post-Scriptum sur les Sociétés de Contrôle*, in *L'autre journal*, 1, 1990, 3-7.

¹³G. FINOCCHIARO, *La sovranità digitale*, in *Diritto pubblico*, 3, 2022; G. HULKÓ, J. KÁLMÁN, A. LAPSÁNSZKY, *The politics of digital sovereignty and the European Union's legislation: navigating crises*, in *Frontiers in Political Science*, 7, 2025, 1548562; M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, 4(1), 2022, 47-51; V. BERTOLA, *La sovranità digitale e il futuro di Internet*, in *Rivista italiana di informatica e diritto*, 2022.

¹⁴A. AYDIN, T.K. BENSGHIR, *Digital data sovereignty: towards a conceptual framework*, in *2019 1st International Informatics and Software Engineering Conference (UBMYK)*, 2019, 1-6; P. HUMMEL, M. BRAUN, M. TRETTER, P. DABROCK, *Data sovereignty: A review*, in *Big Data & Society*, 8(1), 2021; A. CHANDER, H. SUN (a cura di), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford, 2023; G. FINOCCHIARO, *Data and Digital Sovereignty*, cit., 9-12.

¹⁵C. COLAPIETRO, A. MORETTI, *L'intelligenza artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2020, 359-387.

¹⁶L. FLORIDI, *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Cham, 2015.

¹⁷Regolamento (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 (GDPR), GU L 119, 4.5.2016, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Si veda G. SARTOR, F. LAGIOIA, *The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, European Parliamentary Research Service, PE 641.531, 2020.

¹⁸S. ZUBOFF, *The Age of Surveillance Capitalism*, cit.; M. HILDEBRANDT, *Smart Technologies and the End(s) of Law*, Cheltenham, 2015.

governance pubblica¹⁹. La persistente opacità nei processi di raccolta e utilizzo espone gli individui a violazioni della riservatezza²⁰, a rischi securitari e a forme di sorveglianza diffusa, mentre la trasformazione dell'informazione da funzione descrittiva a *potenza performativa* rivela l'inadeguatezza di un paradigma regolatorio fondato esclusivamente sulla tutela della privacy²¹. I sistemi di *machine learning* e le pratiche di *big data analytics* assumono così il ruolo di infrastruttura operativa dei processi di classificazione, ordinamento e personalizzazione dell'informazione, che cessa di fungere da mero ausilio decisionale per assumere la qualità di *impianto cognitivo egemonico* della governance *data-driven*²², plasmando gli habitus sociali e ridefinendo i processi di genesi e redistribuzione del valore economico²³. È in questo quadro che la categoria di *sovranità informazionale*²⁴, intesa come capacità normativa di governare la produzione, la circolazione e l'impiego del dato quale fattore strutturale dell'esercizio del potere, e che nel dominio geopolitico si proietta nella *digital data sovereignty*, ossia nella contesa tra Stati e piattaforme transnazionali per il controllo giurisdizionale sui flussi informativi²⁵, si delinea come ambito concettuale autonomo rispetto alla *data protection*²⁶. Essa non si esaurisce nella tutela individuale dei dati personali, ma ricomprende il controllo sui flussi informativi, il presidio normativo degli ecosistemi algoritmici e la salvaguardia della legittimazione democratica dei processi decisionali automatizzati. Questo scenario pone gli Stati nazionali in una competizione asimmetrica con attori privati transnazionali che esercitano un controllo reale sulle infrastrutture critiche²⁷, generando frizioni tra sovranità statale, logiche economiche e tutela dei diritti fondamentali in un ecosistema transgiuridico caratterizzato da sistemi decisionali opachi e difficil-

¹⁹S. FARO, T.E. FROSINI, G. PERUGINELLI, *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2019; Regolamento (UE) 2022/868 (Data Governance Act), art. 1; Commissione europea, *A European Strategy for Data*, COM 2020 66 final, <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0066>.

²⁰R. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 3, 2013, 587-608. F. PAOLUCCI, *Constitutional Safeguards in the Age of AI. A Study on the Fundamental Rights Impact Assessment of Facial Recognition Technology*, tesi di dottorato, Università Bocconi, Milano, 2025, <https://hdl.handle.net/11565/4074069>.

²¹Sulla critica al paradigma privacy-individuale, cfr. V. RICCIUTO, *L'equivoco della privacy. Persona vs. dato personale*, in *Diritto civile contemporaneo*, 2019.

²²M. HILDEBRANDT, *Law as Information in the Era of Data-Driven Agency*, in *Modern Law Review*, 79(1), 2016, 1-30.

²³G. BEI, rec. di N. SRNICEK, *Platform Capitalism*, in *Annali del Dipartimento di metodi e modelli per l'economia, il territorio e la finanza*, 2023, 153-154.

²⁴N. GILLIBRAND, C. DRAPER, *Informational sovereignty: A new framework for AI regulation*, in *International Journal of Online Dispute Resolution*, 10, 2023, 60.

²⁵R. POLČÁK, D.J.B. SVANTESSON, *Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law*, Cheltenham, 2017, 2: i dati non rappresentano soltanto parte integrante dell'identità individuale, ma anche dell'identità degli Stati, e il controllo su di essi è parimenti necessario tanto per i singoli quanto per le istituzioni sovrane per preservare la propria esistenza; G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE Online*, 57(1), 2023, che analizza il conflitto tra sistemi giuridici nella contesa per la sovranità digitale tra UE, USA e Cina, evidenziando come la *digital data sovereignty* costituisca la dimensione geopolitica e conflittuale di una più ampia sovranità informazionale.

²⁶Sul paradigma della *data protection* come categoria autonoma rispetto alla sovranità informazionale, cfr. P. DE HERT, S. GUTWIRTH, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in E. CLAES et al. (a cura di), *Privacy and the Criminal Law*, Antwerp, 2006, 61-104; V. RICCIUTO, *op. cit.*: la tutela del dato personale risponde a una logica individuale-difensiva che non può esaurire le esigenze di governo strutturale dei flussi informativi su scala sistemica.

²⁷M. TADDEO, *Cyber conflicts and political power in information societies*, in *Minds and Machines*, 27(2), 2017, 265-268.



mente sindacabili²⁸. Sintomatica di questa tensione è la posizione dell'Unione europea, il cui discorso sulla sovranità digitale oscilla tra approccio programmatico e declinazione tecnologica senza tradursi in categorie giuridiche determinate, generando un concetto ancora ambiguo²⁹ che rende difficoltosa la valutazione oggettiva delle politiche implementate³⁰ e che rende particolarmente urgente il rispetto dei principi di trasparenza e *accountability* sanciti dal GDPR e ribaditi dall'AI Act³¹.

L'impiego sistematico di sistemi algoritmici nell'esercizio di funzioni pubbliche, esemplificato da strumenti di *risk assessment* individuale come COMPAS, impiegato per la valutazione del rischio di recidiva³² e da sistemi di predictive policing come *PredPol*, orientati alla previsione spaziale e temporale dei reati³³, accresce il rischio di deresponsabilizzazione sistemica, poiché il potere tende a occultarsi nella neutralità apparente della tecnica. L'autodeterminazione informativa esige allora non solo il consenso, ma anche intelligibilità, accessibilità cognitiva e possibilità effettiva di sindacare i processi automatizzati, senza le quali viene meno la stessa condizione di una partecipazione democratica realmente consapevole. La *data protection* si rivela così strutturalmente incapace di governare un'elaborazione algoritmica che sovverte i principi democratici³⁴ attraverso modelli predittivi che amplificano *bias* preesistenti³⁵, sfruttano vulnerabilità emotive³⁶ e generano una «realità proxy»³⁷, un livello intermedio tra soggetto e reale in cui l'informazione è filtrata e ordinata da logiche non immediatamente intelligibili³⁸, ridefinendo *ex ante* le condizioni di possibilità dell'esperienza cognitiva³⁹ e alimentando *filter bubbles*⁴⁰ ed *echo chambers*⁴¹ che im-

²⁸H. ROBERTS, *Digital sovereignty and artificial intelligence: a normative approach*, in *Ethics and Information Technology*, 26(4), 2024, 70.

²⁹Sul concetto di sovranità digitale e la sua ambivalenza, cfr. N. PALLADINO, *The Ambiguity of Digital Sovereignty between Territorialization of the Cyberspace, Extraterritorial Claims and Digital Rights: Analysing Data Transfer Policies in EU, US and China*, 2023.

³⁰H. ROBERTS, J. COWLS, F. CASOLARI, J. MORLEY, M. TADDEO, L. FLORIDI, *Safeguarding European values with digital sovereignty: an analysis of statements and policies*, in *Internet Policy Review*, 10(3), 2021.

³¹Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act), GUUE, L 2024/1689, 12 luglio 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

³²J. ANGIN, J. LARSON, S. MATTU, L. KIRCHNER, *Machine Bias*, in *ProPublica*, 23 maggio 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (last visited 23/06/2026); S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020.

³³K. LUM, W. ISAAC, *To Predict and Serve?* in *Significance*, 13(5), 2016, 14-19.

³⁴C. O'NEIL, *Weapons of math destruction: How big data increases inequality and threatens democracy*, New York, 2017.

³⁵S. NOBLE, *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York, 2018; D. TALIA, *L'impero dell'algoritmo. L'intelligenza delle macchine e la forma del futuro*, Soveria Mannelli, 2021.

³⁶N. ABOKHODAIR, Y. SKOP, S. RÜLLER, K. AAL, H. ELMIMOUNI, *Opaque algorithms, transparent biases: Automated content moderation during the Sheikh Jarrah Crisis*, in *First Monday*, 2024.

³⁷L. FLORIDI, *The fourth revolution: How the infosphere is reshaping human reality*, Oxford, 2014; Id., *Soft ethics, the governance of the digital and the General Data Protection Regulation. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133), 20180081.

³⁸D. TALIA, *La società calcolabile e i big data: algoritmi e persone nel mondo digitale*, Soveria Mannelli, 2018; Id., *Il potere disciplinare della governamentalità digitale*, in *Rivista di Digital Politics*, 2023.

³⁹D. BEER, *The Data Gaze: Capitalism, Power and Perception*, London, 2018.

⁴⁰E. PARISER, *The Filter Bubble: What the Internet is Hiding from You*, London, 2011.

⁴¹C.R. SUNSTEIN, *Republic: Divided Democracy in the Age of Social Media*, Princeton, 2018; E. BAKSHY, S. MESSING, L.A. ADAMIC, *Exposure to ideologically diverse news and opinion on Facebook*, in *Science*, 348(6239), 2015, 1130-1132; M.

poveriscono la funzione deliberativa dello spazio pubblico⁴² con il supporto di modelli economici orientati alla massimizzazione dell'*engagement*⁴³ e delle logiche di capitalismo della sorveglianza⁴⁴.

Per evitare sovrapposizioni concettuali, è opportuno distinguere tre piani solo in parte coincidenti. La *data protection*, nella ricostruzione consolidata del diritto europeo, opera come tecnica di tutela della persona rispetto al trattamento dei dati personali e si fonda sui principi di liceità, correttezza, limitazione della finalità, minimizzazione e accountability⁴⁵. La *sovranità informazionale* rinvia invece a una dimensione più ampia, che investe la capacità di un ordinamento di governare i flussi informativi e di incidere sulle condizioni strutturali di produzione, circolazione e utilizzo del dato come fattore di potere pubblico⁴⁶. La *digital data sovereignty*, infine, designa la proiezione geopolitica di tale problema e indica la contesa per il controllo delle infrastrutture digitali, degli standard tecnici e dei flussi transfrontalieri di dati⁴⁷. Questi livelli, sebbene interrelati, non coincidono. Un'attenzione esclusiva alla conformità in materia di protezione dei dati rischia di circoscrivere il problema del governo digitale, oscurando questioni più ampie di legittimazione democratica, trasparenza e responsabilità che il costituzionalismo digitale solleva. Sul piano giurisprudenziale si fa breve riferimento alla saga Schrems, su cui ci soffermeremo nei paragrafi successivi. La vicenda mostra come la posta in gioco trascenda la tutela dei dati personali e investa la tenuta delle garanzie strutturali dell'ordinamento di fronte ai poteri digitali, prospettiva che il paragrafo 5 sviluppa in chiave sistematica.

3. Dal dato al potere. Opacità algoritmica, sovranità informazionale e *governance* costituzionalmente orientata

L'opacità dei sistemi basati su reti neurali profonde non costituisce un difetto contingente, ma una caratteristica strutturale dei modelli di apprendimento automatico⁴⁸, che rende la tutela dei dati personali necessaria ma insufficiente a garantire la responsabilità e la legittimazione dei processi decisionali automa-

CINELLI *et al.*, *The echo chamber effect on social media*, *Proceedings of the national academy of sciences*, 118(9), e2023301118, 2021.

⁴²J. HABERMAS, *Ein neuer Strukturwandel der Öffentlichkeit und die deliberative Politik*, Berlin, 2022.

⁴³N. CHOMSKY, E. HERMAN, *Manufacturing Consent: The Political Economy of the Mass Media*, New York, 1989. G. SAMUEL, G.E. DERRICK, T. VAN LEEUWEN, *The ethics ecosystem: Personal ethics, network governance and regulating actors governing the use of social media research data*. *Minerva*, 57(3), 317-343; G. ZICCARDI, *L'odio online: violenza verbale e ossessioni in rete*, Vol. 102, Milano, 2016.

⁴⁴S. ZUBOFF, *The Age of Surveillance Capitalism*, cit.

⁴⁵ Ai sensi dell'art. 5, par. 1, del Regolamento (UE) 2016/679 (GDPR), <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, il trattamento dei dati personali deve conformarsi ai principi di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, mentre il par. 2 consacra il principio di responsabilizzazione del titolare del trattamento. Si veda di P. DE HERT, S. GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in S. GUTWIRTH, Y. POULLET, P. DE HERT (a cura di), *Reinventing Data Protection?*, Dordrecht, 2009, 3-44.

⁴⁶ R. POLČÁK, D.J.B. SVANTESSON, *op. cit.*; N. GILLIBRAND, C. DRAPER, *op. cit.*

⁴⁷ H. ROBERTS, J. COWLS, F. CASOLARI, J. MORLEY, M. TADDEO, L. FLORIDI, *Safeguarding European values with digital sovereignty: An analysis of statements and policies*, in *Internet Policy Review*, 10(3), 2021.

⁴⁸F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Cambridge (MA), 2015.

tizzati⁴⁹ e impone lo sviluppo di strumenti capaci di bilanciare diritti fondamentali e flussi informativi algoritmici⁵⁰. La centralità della *datafication*⁵¹ induce, più in generale, uno slittamento epistemico del potere pubblico in cui la decisione tende a fondarsi sull'efficacia predittiva dei sistemi più che sulla giustificazione razionale⁵², determinando una forma di escalation conflittuale in cui la *digital data sovereignty*, nella sua proiezione di sovranità informazionale, acquisisce una forza determinante nelle logiche di dominio, mentre la *data protection* vede progressivamente ridursi la propria efficacia cogente, erosa da meccanismi opachi e algoritmi di intelligenza artificiale che assorbono anche i dati personali in circuiti di potere difficilmente reversibili. Di fronte a questa diagnosi, la risposta non può essere un correttivo esterno agli algoritmi, ma richiede la riconfigurazione dall'interno delle condizioni di comprensibilità, tracciabilità e controllo. Su questo sfondo si colloca HAIMLA (*Hybrid Artificial Intelligence Methodology for Legal Analysis*)⁵³, un'architettura procedurale a orientamento costituzionale che supera i limiti dei modelli puramente probabilistici⁵⁴ integrando intelligenza artificiale simbolica e sub-simbolica, garantendo l'isomorfismo tra la norma e la sua rappresentazione digitale attraverso un paradigma umanocentrico, fondato su un livello di supervisione giuridica integrata descritto nel dettaglio nel paragrafo seguente, che restituisce alla governance dei sistemi cognitivi automatizzati un presidio normativo attivo e verificabile. HAIMLA potrebbe trasformare i dati in risorse cognitive verificabili, implementando i principi FAIR, *Findable, Ac-*

⁴⁹C. COLAPIETRO, A. MORETTI, *L'intelligenza artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2020, 359-387.

⁵⁰A. DI CORINTO, *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in *Rivista italiana di informatica e diritto*, 4(1), 2022, 31-37.

⁵¹Sul termine *datafication*: V. MAYER-SCHÖNBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, London, 2013, 78; cfr. J. VAN DIJCK, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in *Surveillance & Society*, 12(2), 2014, 197-208; U.A. MEJIAS, N. COULDRY, *Datafication*, in *Internet Policy Review*, 8(4), 2019.

⁵²Esemplificativo il caso *PredPol (predictive policing)*: genera mappe di rischio geospaziale concentrando la presenza poliziesca in aree già marginalizzate. Si vedano: A.G. FERGUSON, *The Rise of Big Data Policing*, New York, 2017; A.D. SELBST, *Disparate impact in big data policing*, in *Georgia Law Review*, 52(109), 2017; A. BONFANTI, «Big data» e polizia predittiva, in *MediaLaws*, 3, 2018, 1-13. Tali sistemi, definiti critici dal Regolamento UE 2024/1689 (AI Act) che ne limita fortemente l'uso, sono stati criticati per l'insufficienza delle tutele basate sulla sola privacy contro la sorveglianza biometrica. Si veda: Brennan Center for Justice, 2022 U.A. MEJIAS, N. COULDRY, *Datafication*, in *Internet Policy Review*, 8, 4.

⁵³M. PALMIRANI, S. SAPIENZA, K. ASHLEY, *A hybrid artificial intelligence methodology for legal analysis*, in *BioLaw Journal – Rivista di BioDiritto*, 3, 2024, 389-409. La metodologia combina *machine learning* con strutture logico-giuridiche formali basate su XML Akoma Ntoso e LegalRuleML, garantendo intelligibilità e sindacabilità delle decisioni automatizzate attraverso un *workflow* con supervisione umana attiva (*human-in-the-loop*). Il modello gestisce variabili critiche quali gli operatori deontici (obblighi, divieti, permessi) e la dinamicità temporale del diritto (*point-in-time*). Il processo si sviluppa attraverso un *workflow* iterativo in sei fasi: dopo una fase preliminare di definizione delle ipotesi e preparazione del corpus, il sistema alterna l'estrazione automatica di fattori e l'intervento umano. Un passaggio fondamentale è la creazione di un «gold standard»: esperti legali annotano manualmente i documenti per istruire l'algoritmo, assicurando che l'addestramento rifletta interpretazioni giuridiche autorevoli e non semplici correlazioni numeriche. Nella fase di validazione, il giurista analizza criticamente la matrice di confusione generata dal sistema valutando la significatività giuridica degli errori (falsi positivi e falsi negativi), uno scrutinio che permette di identificare *bias* o interpretazioni errate, come l'uso di termini gergali o formule tecniche in ambiti di bio-diritto.

⁵⁴L. FLORIDI et al., *AI4People. An ethical framework for a good AI society: opportunities, risks, principles, and recommendations*, in *Minds and Machines*, 28(4), 2018, 689-707.

*cessible, Interoperable, Reusable*⁵⁵, la cui piena coniugazione normativa e applicativa sarà oggetto di approfondimento nel capitolo successivo, come architettura operativa, e sviluppando sistemi *trustworthy-by-design*⁵⁶ capaci di preservare le specificità del sistema giuridico nazionale⁵⁷. Tali soluzioni tecniche, tuttavia, costituirebbero condizione necessaria ma non sufficiente. Soltanto nell'ambito di un sistema di costituzionalismo digitale⁵⁸ in cui la governance algoritmica precede e orienta sia la tecnica sia la normativa intesa come funzione applicativa, è possibile che i principi fondanti del diritto costituzionale si traducano in vincoli cogenti per l'intero impianto digitale. In questo senso, HAIMLA non si limita a correggere l'opacità tecnica dei sistemi, ma traduce in termini procedurali l'esigenza di una sovranità informazionale costituzionalmente orientata.

Sul piano tecnico-giuridico, HAIMLA opera attraverso un'architettura a tre livelli funzionalmente interconnessi. Il primo è un modulo simbolico fondato su ontologie giuridiche formali e regole di inferenza esplicite, che assicura la conformità strutturale alla norma e la tracciabilità di ogni passaggio inferenziale. Ogni decisione può essere ricondotta alla disposizione normativa che la fonda, realizzando l'isomorfismo tra norma e rappresentazione digitale. Il secondo è un modulo sub-simbolico basato su reti neurali addestrate su corpus giuridici annotati semanticamente, che gestisce la variabilità linguistica, l'interpretazione contestuale e le zone di indeterminatezza del linguaggio normativo. Il terzo è un livello di supervisione umana integrata (*human-in-the-loop*), in cui il giurista insieme agli esperti di dominio e agli ingegneri del sistema, non si limita a validare ex post l'output del sistema ma è strutturalmente incorporato nel ciclo di addestramento mediante protocolli di annotazione semantico-giuridica, con il compito di valutare non la mera accuratezza statistica ma la significatività giuridica degli errori⁵⁹.

Questo impianto procedurale risponde alle critiche formulate dalla giurisprudenza comparata sull'uso di sistemi algoritmici nelle decisioni pubbliche. Nel caso *State v. Loomis* (Corte Suprema del Wisconsin, 2016), la Corte aveva ritenuto compatibile l'uso del sistema COMPAS nelle decisioni di condanna penale con il *due process*⁶⁰, subordinandone tuttavia l'uso a tre condizioni: il punteggio di rischio non può essere il fattore determinante della decisione, il giudice deve fornire una motivazione autonoma e non limitata al mero richiamo del risultato algoritmico, e tale risultato non può da solo determinare la severità della

⁵⁵M.D. WILKINSON *et al.*, *op. cit.* I quattro principi – *Findable, Accessible, Interoperable, Reusable* – sono stati elaborati per garantire che le risorse digitali siano accessibili e riutilizzabili tanto da esseri umani quanto da sistemi computazionali. La loro applicazione alla gestione dei dati giuridici nell'ambito di architetture di *legal AI* sarà oggetto di approfondimento nel capitolo successivo.

⁵⁶Con *trustworthy-by-design* si intende un approccio progettuale in cui i requisiti di affidabilità, trasparenza e rispetto dei diritti fondamentali sono incorporati nella struttura del sistema fin dalla fase di sviluppo, anziché aggiunti successivamente. Si veda High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai> (last visited 23/06/2026); Regolamento (UE) 2024/1689 (AI Act), *cit.*

⁵⁷Strategia italiana per l'intelligenza artificiale 2024-2026, https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_intelligenza_artificiale_2024-2026.pdf (last visited 23/06/2026).

⁵⁸G. DE GREGORIO, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022; O. POLLICINO, G. DE GREGORIO, *Constitutional Law in the Algorithmic Society*, in H.-W. MICKLITZ *et al.* (a cura di), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

⁵⁹M. PALMIRANI, S. SAPIENZA, *op. cit.*

⁶⁰Cfr. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S. Ct. 2290 (2017); cfr. S.G. MAYSON, *Bias In, Bias Out*, in *Yale Law Journal*, 128(8), 2019, 2218-2300; B.E. HARCOURT, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, Chicago, 2019.



pena. Un'esigenza di trasparenza procedurale che HAIMLA incorpora come vincolo strutturale. Analoga preoccupazione emerge nelle più recenti politiche federali statunitensi in materia di *Automated Decision Systems* nell'amministrazione pubblica, che richiedono motivazioni che rispecchino il processo decisionale effettivo e non solo il risultato finale. Un requisito coerente con il paradigma HAIMLA di isomorfismo tra norma e rappresentazione digitale, recepito in forma strutturata dall'AI Act europeo (artt. 11–13) per i sistemi ad alto rischio⁶¹.

Se la sovranità digitale costituisce, nel quadro elaborato da Peters⁶², un *protective office* al servizio dell'umanità, HAIMLA ne rappresenta il braccio operativo, vale a dire l'architettura procedurale che traduce il *munus* di protezione in garanzia strutturale e verificabile. I principi FAIR, analizzati nel capitolo seguente, non si aggiungono dall'esterno a questo dispositivo ma ne sono il carburante. Sono i dati FAIR, trovabili, accessibili, interoperabili, riutilizzabili a rendere possibile la trasformazione che HAIMLA opera, convertendo la materia grezza informazionale in conoscenza giuridica auditabile⁶³.

4. I principi FAIR come presidio costituzionale della *governance* algoritmica

Oltre i confini tradizionali degli Stati, la gestione dei dati contribuisce a rimodellare la geografia del potere globale, generando forme di sovranità informazionale di tipo reticolare, in grado di determinare l'accesso alle risorse cognitive attraverso infrastrutture digitali caratterizzate da profili di marcata disparità strutturale. I dati, inizialmente ricondotti alla metafora economica del «nuovo petrolio»⁶⁴, oltrepassano tale inquadramento e assumono una funzione costitutiva dell'ordine giuridico, divenendo infrastrutture normative che mediano l'esperienza umana e le condizioni stesse della governabilità. Questa trasformazione ne intensifica la dimensione estrattiva e si iscrive in dinamiche riconducibili a un neocolonialismo digitale⁶⁵, in cui la captazione massiva di informazioni riconfigura gli individui come fonti di valore informazionale, producendo al contempo accumulazione economica ed egemonia epistemica. La competizione globale si disloca così sulla configurazione dell'ambiente digitale, coinvolgendo piattaforme transnazionali, Stati e aggregati geopolitici nella definizione e nel controllo di infrastrutture, algoritmi e standard protocollari⁶⁶.

⁶¹ F. PASQUALE, *The scored society: Due process for automated predictions*, in *Washington Law Review*, 89(1), 2014; A. ZAVRŠNIK, *Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings*, in *European Journal of Criminology*, 18(5), 2021, 623-642; National Institute of Standards and Technology (NIST), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, Gaithersburg 2023, <https://nvl-pubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> (last visited 23/06/2026).

⁶² A. PETERS, *op. cit.*

⁶³ S. EZE, *From Model-Level Explanations to Legal Evidence: Auditing Bias and Explainability in GDPR-Compliant Automated Decision Systems*, SSRN Working Paper, 2025, <https://ssrn.com/abstract=5783263> (last visited 23/06/2026); B. GOODMAN, S. FLAXMAN, *European Union Regulations on Algorithmic Decision-Making and a «Right to Explanation»*, in *AI Magazine*, 38(3), 2017, 50-57.

⁶⁴ C. STACH, *Data is the new oil – sort of: a view on why this comparison is misleading and its implications for modern data administration*, in *Future Internet*, 15(2), 2023, 71.

⁶⁵ N. COULDRY, U.A. MEJIAS, *Data colonialism: Rethinking big data's relation to the contemporary subject*, in *Television & New Media*, 20(4), 2019, 336-349.

⁶⁶ A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 8(1), 2019, 87-106. F. SERINI, *La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana*, in *Rivista italiana di informatica e diritto*, 2, 2024, 41-76. Su un piano distinto, ma egualmente sintomatico della contesa geo-

In tale quadro di frammentazione e ricomposizione del potere, il diritto sovranazionale è chiamato a riaffermare la propria funzione ordinatrice non come osservatore passivo dell'innovazione tecnologica, ma come principio teleologico in grado di orientare l'evoluzione dell'ordine digitale, preservando la sua capacità di garantire i diritti democratici e la partecipazione dei cittadini ai processi decisionali⁶⁷.

Su questo piano, la protezione dei dati personali si configura come punto di equilibrio dialettico tra libertà e potere, tra tecnica e diritto. In un mondo caratterizzato dalla dissoluzione progressiva dei confini giuridici e culturali nel cosiddetto «villaggio globale»⁶⁸, il controllo sui propri dati diventa il perno di una cittadinanza effettiva e della tutela dei diritti fondamentali⁶⁹, ancorando l'esercizio del potere tecnologico a principi democratici condivisi. È precisamente in questo snodo che i principi FAIR, elaborati nel contesto della scienza aperta al fine di garantire qualità, tracciabilità e replicabilità dei dati scientifici, assumono una statura epistemica e normativa tale da elevarli a fondamento strutturale di una governance algoritmica democraticamente legittimata⁷⁰. In entrambi i domini ciò che è in gioco è la condizione di possibilità del controllo intersoggettivo. La replicabilità del dato scientifico e la sindacabilità della decisione algoritmica condividono la medesima struttura normativa fondamentale, ossia la pretesa che il processo attraverso cui si giunge a un risultato sia accessibile, comprensibile e contestabile da parte di soggetti terzi. Se la legittimità della scienza moderna riposa sulla pubblicità del metodo, la legittimità democratica dell'esercizio del potere riposa sulla pubblicità delle ragioni – questi criteri operano precisamente come dispositivi di pubblicità applicati all'infrastruttura cognitiva del potere algoritmico, traducendo in parametri tecnici la pretesa costituzionale di trasparenza e *accountability*. Non si tratta pertanto di esportare acriticamente un vocabolario della gestione dei dati scientifici verso il diritto costituzionale, ma di riconoscere che tale framework codifica, sul piano tecnico-operativo, quelle medesime esigenze di intelligibilità e verificabilità che il costituzionalismo esprime sul piano normativo-valoriale. Il loro valore aggiunto risiede nella capacità di tradurre tali esigenze in vincoli progettuali concreti, operanti *ab initio* nella fase di costruzione dei sistemi algoritmici, secondo una logica di *by design* che il diritto europeo già conosce e valorizza. Nel contesto delle profonde trasformazioni che ridefiniscono l'esercizio dei diritti fondamentali nell'ecosistema digitale, questi strumenti si distinguono per la loro rilevanza sistemica, operando come matrici di razionalizzazione giuridico-tecnica dell'architettura algoritmica e offrendo un quadro di orientamento volto a garantire sia la tutela sostanziale dei diritti sia la legittimazione democratica dei processi decisionali automatizzati⁷¹. Quando i dati alla base dei modelli generativi sono gestiti secondo tali criteri, essi si trasfor-

politica sulle infrastrutture digitali, si veda Conclusioni dell'Avvocato generale Ćapeta, 19 marzo 2026, causa C-354/24, *Elisa Eesti AS c. Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu e Tarbijakaitse ja Tehnilise Järelevalve Amet*, EU:C:2026:222, relativa all'esclusione di apparati di telecomunicazione extra-UE per motivi di sicurezza nazionale, che pone questioni di proporzionalità analoghe a quelle qui discusse, sebbene sul terreno della sicurezza delle infrastrutture piuttosto che della protezione dei dati personali.

⁶⁷ S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 1, 2019, 63-89.

⁶⁸ M. McLuhan, *Understanding Media: The Extensions of Man*, Cambridge (MA), 1994.

⁶⁹ G. DE MINICO, *Fundamental rights. European digital regulation and algorithmic challenge*, in *European Business Law Review*, 2021; S. LISSENS, *The Foundations of EU Personal Data Protection Law: Privacy and Human Dignity*, 2024.

⁷⁰ M.D. WILKINSON *et al.*, *op. cit.*

⁷¹ E.G. HERNÁNDEZ, *Towards an ethical and inclusive implementation of artificial intelligence in organizations: a multidimensional framework*, 2024.

mano in strumenti controllabili, verificabili e idonei a fondare sistemi di IA generativa responsabili⁷². Lo schema in esame trasforma i dati da semplici informazioni grezze in beni informativi verificabili e contestabili. *Findable*, attraverso metadati ricchi e identificatori persistenti; *Accessible*, mediante protocolli standardizzati e politiche di accesso trasparenti; *Interoperable*, grazie a vocabolari condivisi e formati uniformi; *Reusable*, attraverso licenze esplicite e documentazione completa. Operando lungo l'intero ciclo di vita del dato, questo approccio rende intelligibili le logiche computazionali e ne consente un vaglio critico e democraticamente informato. Tale paradigma *FAIR by design*⁷³, in continuità con il principio di *privacy by design* sancito dal GDPR (art. 25)⁷⁴, si intreccia con l'architettura normativa europea, l'*AI Act*⁷⁵ ne recepisce la logica per sistemi ad alto rischio; il *Data Governance Act*⁷⁶ e il *Data Act*⁷⁷ ne istituzionalizzano l'applicazione; standard come EUCS e ISO/IEC 42001⁷⁸ ne traducono i requisiti in parametri operativi. Se la qualità democratica dei sistemi algoritmici non si misura soltanto in termini di efficienza, ma nella possibilità di comprenderli e metterli in discussione, essa dipende da come dati e processi vengono strutturati. È su questo piano che la sovranità informativa smette di configurarsi come monopolio degli Stati o delle grandi piattaforme e si redistribuisce tra cittadini consapevoli, titolari di diritti cognitivi e digitali. In questa configurazione, l'informazione non è più una risorsa estrattiva, ma una condizione operativa della libertà e della responsabilità condivisa⁷⁹. Per chiarire come questi requisiti epistemici si traducano in vincoli progettuali già presenti o in nuce nel panorama normativo europeo, la Tabella 1 sintetizza la correlazione tra i principi FAIR e il loro ancoraggio costituzionale.

Tabella 1. I principi FAIR come architettura costituzionale della *governance* algoritmica

Principio FAIR	Definizione operativa	Correlato costituzionale	Riferimenti normativi EU
<i>Findable</i>	Metadati ricchi e identificatori persistenti che rendono i dati rintracciabili da sistemi e persone	Pubblicità e accessibilità degli atti; obbligo di motivazione degli algoritmi pubblici	Art. 13 GDPR; art. 13 AI Act; Open Data Directive 2019/1024

⁷² A. BATTOOL, D. ZOWGHI, M. BANO, *Responsible AI governance: a systematic literature review*, 2023.

⁷³ E. SORRENTINO, A.F. SPAGNUOLO, *op. cit.*

⁷⁴ Il principio di *FAIR by design* implica l'incorporazione dei criteri FAIR nelle prime fasi di progettazione di piattaforme e infrastrutture, in continuità con l'approccio *privacy by design*. Il concetto è elaborato in: M.D. WILKINSON *et al.*, *op. cit.*

⁷⁵ Regolamento (UE) 2024/1689 (*AI Act*), *cit.*

⁷⁶ Regolamento (UE) 2022/868 (*Data Governance Act*), *cit.*; Commissione europea, *Data Governance Act Explained*, 2024, <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained> (last visited 23/06/2026).

⁷⁷ 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 (*Data Act*), in vigore dall'11 gennaio 2024, applicabile dal 12 settembre 2025, in *GUUE*, L 2023/2854, 22 dicembre 2023.

⁷⁸ ENISA, *European Union Cybersecurity Certification Scheme for Cloud Services (EUCS)*, 2024.

ISO/IEC 42001:2023, *Information Technology – Artificial Intelligence – Management System*, Ginevra 2023.

⁷⁹ J.D. WEISZ, M. MULLER, J. HE, S. HOUE, *Toward general design principles for generative AI applications, Applications*, in *arXiv preprint*, 2023.

<i>Accessible</i>	Protocolli standardizzati (API aperte) e politiche di accesso trasparenti, anche per dati ad accesso limitato	Diritto di accesso ex art. 15 GDPR; diritto all'esplicabilità nelle decisioni automatizzate (art. 22 GDPR)	Data Governance Act; Art. 13 AI Act; art. 25 GDPR (privacy by design)
<i>Interoperable</i>	Vocabolari condivisi, ontologie formali e formati uniformi per l'integrazione tra sistemi diversi	Interoperabilità dei sistemi pubblici; non discriminazione per standard tecnici	Data Act (artt. 33, 35, 36); EUCS; ISO/IEC 42001; Reg. (UE) 2018/1724
<i>Reusable</i>	Licenze esplicite, provenienza documentata e contesto di raccolta per il riutilizzo legittimo	Portabilità ex art. 20 GDPR; limitazione della finalità; divieto di profilazione discriminatoria	Data Act (art. 5); Digital Services Act; AI Act (requisiti qualità dati, art. 10)

Su questo sfondo, il nesso tra principi FAIR, metodologia HAIMLA e costituzionalismo digitale diventa più netto. *Findability* e *Accessibility* realizzano la condizione di pubblicità del metodo che il costituzionalismo tradizionale esige dall'atto pubblico e che nell'ecosistema algoritmico si traduce nella tracciabilità degli input e dei parametri decisionali; *Interoperability* garantisce la verificabilità esterna, ossia la possibilità per soggetti terzi (autorità di controllo, giudici, ricercatori) di replicare e contestare i risultati; *Reusability* fonda la continuità della supervisione democratica nel tempo, impedendo che l'opacità si accumuli attraverso aggiornamenti successivi del sistema. HAIMLA integra questi quattro requisiti come vincoli architeturali. Il modulo simbolico garantisce *Findability* e *Interoperability* attraverso ontologie formali; il modulo sub-simbolico è addestrato su dati *Reusable* e documentati; la supervisione umana assicura l'*Accessibility* cognitiva del processo decisionale per i destinatari della norma. I dati strutturati secondo i principi FAIR costituiscono come già anticipato la materia prima epistemica che HAIMLA trasforma in conoscenza verificabile e auditabile. Senza tale fondamento strutturale, il sindacato algoritmico resterebbe privo di substrato cognitivo adeguato.

5. Costituzionalismo digitale e i confini del paradigma regolatorio tradizionale

Le analisi svolte nei capitoli precedenti consentono di formulare, a questo punto, una tesi di sintesi. Il potere algoritmico si è costituito come nuova forma di sovranità infrastrutturale, capace di condizionare la formazione delle preferenze collettive e di incidere sulla distribuzione effettiva dei diritti fondamentali, operando al di fuori, e spesso al di là, dei circuiti tradizionali di legittimazione democratica. La *data protection*, per quanto necessaria, e gli strumenti regolativi procedurali, per quanto opportuni, non bastano a fronteggiare questa trasformazione di fondo. Essi presuppongono un potere già identificato, localizzato e sindacabile, condizioni che la governance algoritmica sistematicamente disattende. Occorre dunque



compiere un salto qualitativo, superando l'idea di un diritto che interviene ex post sulle patologie e orientandolo a modellare *ab initio* le condizioni di funzionamento dell'ecosistema digitale. In questo orizzonte, il costituzionalismo digitale⁸⁰ non si limita a descrivere la realtà, ma assume una funzione genuinamente paradigmatica. Non si riduce a un'estensione del diritto pubblico classico nello spazio tecnologico. Comporta invece una ridefinizione dei soggetti, delle fonti e dei rimedi del diritto costituzionale. I soggetti, perché le grandi piattaforme e i sistemi di intelligenza artificiale non sono semplici destinatari della norma ma veri progettisti di regole endogene capaci di orientare comportamenti collettivi con un'intensità comparabile a quella del diritto positivo⁸¹. Le fonti, perché gli standard tecnici e le architetture by design acquisiscono una funzione normativa sostanziale che il diritto deve riconoscere e disciplinare, non ignorare o subire⁸². I rimedi, perché la tutela effettiva dei diritti non può affidarsi soltanto all'impugnazione giurisdizionale ex post di singoli atti lesivi e richiede invece meccanismi di verifica sull'architettura dei sistemi, incorporati nel loro ciclo di vita prima che le conseguenze si materializzino⁸³.

In questa prospettiva, l'evoluzione normativa europea, dall'*AI Act* al *Data Governance Act*, dal DSA⁸⁴ al DMA⁸⁵, rappresenta non tanto un sistema regolatorio compiuto quanto l'emersione progressiva, ancora disorganica, di un nuovo paradigma ovvero quello di un diritto che ambisce a configurare le condizioni di esercizio del potere digitale, anziché limitarsi a sanzionarne le degenerazioni. In tale quadro, i principi FAIR e la metodologia HAIMLA, di cui si è già illustrata la dimensione tecnico-operativa, rilevano qui nella loro valenza giuridico-costituzionale. Essi traducono in vincoli progettuali concreti le medesime esigenze di intelligibilità e sindacabilità che il costituzionalismo esprime sul piano normativo. Il nesso non è analogico, ma funzionale. I dati FAIR costituiscono il presupposto epistemico senza cui HAIMLA non può operare. La rintracciabilità e l'interoperabilità dei dataset di addestramento sono condizioni di possibilità per la supervisione giuridica nel ciclo inferenziale; la *Reusability* documentata fonda la continuità dell'audit nel tempo. Reciprocamente, HAIMLA traduce in vincoli procedurali verificabili le esigenze che i principi FAIR esprimono in termini epistemici. L'isomorfismo tra norma e rappresentazione digitale, garantito dal modulo simbolico, è la forma giuridica dell'esigenza di dati *Findable* e *Interoperable*. Il cerchio si chiude nel costituzionalismo digitale, che fornisce la cornice normativa entro cui tali vincoli assumono forza cogente. L'obbligo di motivazione dell'atto amministrativo automatizzato, già affermato dalla giurisprudenza del

⁸⁰ G. DE GREGORIO, R. RADU, *Digital constitutionalism in the new era of Internet governance*, in *International Journal of Law and Information Technology*, 30(1), 2022, 68-87.

⁸¹ O. POLLICINO, *Costituzionalismo digitale. Pensare la democrazia al tempo dell'AI*, Bologna, 2025; Id., *Di cosa parliamo quando parliamo di costituzionalismo digitale?* in *Quaderni costituzionali*, 3, 2023.

⁸² O. POLLICINO, G. DE GREGORIO, *Constitutional Democracy in the Age of Algorithms: The Implications of Digital Private Powers on the Rule of Law in Times of Pandemics*, 2020; G. DE GREGORIO, *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*, Cambridge, 2022.

⁸³ T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informazione e dell'informatica*, 3, 2020, 465-484; E. LONGO, A. PIN, *Oltre il costituzionalismo? Nuovi principi e regole costituzionali per l'era digitale*, in *Diritto pubblico comparato ed europeo*, 25(1), 2023, 103-116.

⁸⁴ 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 (*Digital Services Act*), in *GUUE*, L 277, 27 ottobre 2022.

⁸⁵ 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 (*Digital Markets Act*), in *GUUE*, L 265, 12 ottobre 2022.

Consiglio di Stato⁸⁶, e la trasparenza cognitiva dei sistemi algoritmici condividono la medesima pretesa di fondo che l'esercizio del potere sia verificabile e contestabile da parte di soggetti terzi. Sul piano della giurisprudenza sovranazionale, tale convergenza emerge con chiarezza nella saga Schrems, pur con un esito recente che introduce un elemento di discontinuità. Se la sentenza C-362/14 del 2015 ha invalidato il *Safe Harbour*⁸⁷ e la sentenza C-311/18 del 2020 ha travolto il *Privacy Shield*⁸⁸, sulla base di un sindacato rigoroso sul «livello di protezione sostanzialmente equivalente» richiesto ai paesi terzi, la pronuncia T-553/23 del Tribunale dell'Unione europea del 3 settembre 2025 ha invece respinto il ricorso proposto contro la decisione di adeguatezza relativa al *Data Privacy Framework* USA-UE, pur introducendo una diversa valutazione circa l'adeguatezza delle garanzie statunitensi. Nello specifico il Tribunale ha ritenuto che la Commissione potesse legittimamente concludere, nell'esercizio del proprio margine di valutazione, per la sussistenza di un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione, in considerazione dell'assetto complessivo dei meccanismi statunitensi di sorveglianza e di ricorso⁸⁹. Tale esito, che segnala un possibile parziale allontanamento dal rigore delle precedenti pronunce Schrems, non sembra tuttavia incidere sul dato strutturale qui rilevante. Anche nel confermare l'adeguatezza, il giudice europeo è stato chiamato a valutare l'effettività e l'indipendenza dei meccanismi di controllo nel loro complesso, secondo un parametro che va oltre la sola dimensione della tutela individuale dei dati personali e che tocca anche la legittimazione istituzionale del potere informativo. In attesa di un eventuale vaglio della Corte di giustizia in sede di impugnazione, questa tensione rappresenta il banco di prova del costituzionalismo digitale ovvero verificare se il controllo giurisdizionale ex post sia effettivamente in grado di compensare le asimmetrie informative generate dai sistemi tecnologici e dai meccanismi di sorveglianza transnazionali.

A questo interrogativo il presente lavoro non offre una risposta risolutiva: va riconosciuto, infatti, che il paradigma proposto non elimina le tensioni che attraversano la governance algoritmica, ma le assume come condizioni permanenti entro cui operare. Permangono, in particolare, due limiti strutturali: l'asimmetria cognitiva tra istituzione e sistema, che richiede autorità di controllo adeguatamente attrezzate e magistrature capaci di valutare la correttezza giuridica, e non soltanto la precisione statistica, delle decisioni automatizzate; e la frammentazione geopolitica degli standard tecnici, che i sistemi algoritmici trans-

⁸⁶ Cfr. Cons. Stato, Sez. VI, 8 aprile 2019, n. 2270, che ha equiparato l'algoritmo all'atto amministrativo elettronico, stabilendo che la digitalizzazione non può giustificare l'elusione dei principi di trasparenza e motivazione; Cons. Stato, Sez. VI, 13 dicembre 2019, n. 8472, che ha sancito il principio di «piena conoscibilità» del modulo software e della regola tecnica sottostante; Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881, secondo cui la motivazione deve tradurre la formula tecnica in regola giuridica comprensibile. Per un inquadramento teorico e costituzionale della materia, si vedano E. LONGO, *Giustizia digitale e Costituzione. Riflessioni sulla trasformazione tecnica della funzione giurisdizionale*, Milano, (2023), 1-391.; A. SIMONCINI, *Il linguaggio dell'intelligenza artificiale e la tutela costituzionale dei diritti*, in *Rivista AIC*, 2023, 1-38.

⁸⁷ Corte giust. UE, 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner (Safe Harbour)*, EU:C:2015:566.

⁸⁸ Corte giust. UE, 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximilian Schrems (Privacy Shield)*, EU:C:2020:559.

⁸⁹ Trib. UE, 3 settembre 2025, causa T-553/23, *Latombe c. Commissione europea (Data Privacy Framework)*, EU:T:2025:831



nazionali attraversano con disinvoltura⁹⁰. Proprio per questo, la risposta più coerente non è un incremento quantitativo di regolazione, ma un modello di *governance* adattiva che assuma la propria incompletezza come condizione di legittimità e in cui la revisione periodica dei parametri algoritmici, l'intelligibilità delle decisioni automatizzate come presupposto della loro sindacabilità e la *co-regulation* tra autorità pubbliche, operatori e società civile non siano soluzioni definitive, ma le condizioni minime affinché il costituzionalismo digitale possa operare come sistema aperto, capace di adeguarsi all'evoluzione tecnica senza perdere il proprio ancoraggio ai principi fondanti.

Questa prospettiva impone di ripensare il rapporto tra costituzionalismo e tecnica non come conflitto tra due logiche antagoniste, ma come tensione produttiva da governare. La digitalizzazione dell'esperienza pubblica non rappresenta una traiettoria necessaria e predeterminata, ma un fenomeno suscettibile di indirizzo attraverso il diritto e le istituzioni democratiche. I principi di autonomia, uguaglianza, pluralismo informativo e partecipazione non si pongono in rapporto di incompatibilità con la razionalità algoritmica, ma esigono di essere incorporati nelle regole e nelle procedure che governano la progettazione e l'operatività dei sistemi digitali⁹¹. Standard FAIR, audit algoritmici, protocolli di interoperabilità e meccanismi di *legal protection by design*⁹² non risolvono integralmente le criticità poste dal potere algoritmico, ma contribuiscono a ricondurle entro uno spazio nel quale il controllo democratico può esercitarsi in modo effettivo e informato. La legittimazione democratica dei sistemi algoritmici non dipende primariamente dalla loro efficienza, bensì dal grado di intelligibilità e sindacabilità che essi garantiscono: presuppone che cittadini, istituzioni e operatori del diritto siano posti nelle condizioni di comprendere le logiche di funzionamento dei sistemi, le ragioni delle decisioni prodotte e le modalità attraverso cui tali decisioni possano essere sottoposte a verifica e contestazione.

6. Conclusioni

La trasformazione digitale ha dato origine a una configurazione della sovranità profondamente diversa da quella affermata nella modernità politica. Il potere non si esercita più principalmente attraverso il controllo del territorio o delle istituzioni tradizionali, ma mediante il governo dei flussi informativi e delle infrastrutture cognitive che rendono possibile la stessa costruzione del significato sociale. La progressiva *datafication* dell'esperienza umana alimenta un regime epistemico nel quale la produzione della cono-

⁹⁰R. GUIDOTTI, A. MONREALE, S. RUGGIERI *et al.*, *A Survey of Methods for Explaining Black Box Models*, in *ACM Computing Surveys*, 51(5), 2019, art. 93, 1-42; B. GOODMAN, S. FLAXMAN, *European Union Regulations on Algorithmic Decision-Making and a «Right to Explanation»*, in *AI Magazine*, 38(3), 2017, 50-57.

⁹¹M. BETZU, *I poteri privati nella società digitale: oligopoli e antitrust*, in *Diritto pubblico*, 27(3), 2021, 739-760. M. BASSINI, *Internet e libertà di espressione: prospettive costituzionali e sovranazionali*, Roma 2019; A. SIMONCINI, *L'algoritmo incostituzionale*, cit.; E. LONGO, *La giustizia nell'era digitale*, cit.

⁹²Il concetto di *legal protection by design* designa l'incorporazione di garanzie giuridiche e tutele dei diritti fondamentali direttamente nell'architettura tecnica dei sistemi digitali, in fase di progettazione e non come correttivo successivo. Il paradigma è elaborato in G. DE GREGORIO, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022; O. POLICINO, *Costituzionalismo digitale. Pensare la democrazia al tempo dell'IA*, Bologna, 2025. In senso convergente, con riferimento al principio di privacy by design come archetipo normativo, v. A. CAVOUKIAN, *Privacy by Design: The 7 Foundational Principles*, Information and Privacy Commissioner of Ontario, Toronto 5, 2009, 12; A. SIMONCINI, *L'algoritmo incostituzionale*, cit., 63-89; E. LONGO, *La giustizia nell'era digitale*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica. Atti del Convegno Annuale dell'Associazione «Gruppo di Pisa»*, Napoli, 2022, 161-205.

scienza tende a essere subordinata alle logiche della predizione algoritmica e i criteri di verità vengono progressivamente ricondotti a forme di correlazione computazionale. In questo contesto, individui e collettività rischiano di essere ridotti a insiemi di dati suscettibili di estrazione, aggregazione e valorizzazione, al servizio di finalità economiche, strategie di controllo e dinamiche di competizione geopolitica. L'impianto teorico qui delineato, fondato sulla riconcettualizzazione della sovranità come *protective office*, sull'impiego dei principi FAIR come presidi strutturali e sull'HAIMLA come dispositivo procedurale di governo dell'innovazione, rinvia a una precondizione normativa di carattere generale. Tale precondizione concerne la possibilità che emergano soggettività in grado di rendere intelligibili le forme del potere algoritmico e di incidere criticamente sui processi della sua organizzazione, legittimazione e riproduzione. L'autodeterminazione informativa, in questa prospettiva, trascende la tradizionale tutela della riservatezza per configurarsi come fondamento della cittadinanza digitale: il controllo consapevole sui propri dati diviene precondizione imprescindibile per partecipare, comprendere e legittimamente contestare i processi algoritmici che strutturano l'esperienza sociale⁹³. Sul piano delle *policy*, l'architettura proposta suggerisce indicazioni operative concrete. Il recepimento dell'*AI Act* negli ordinamenti nazionali dovrebbe essere accompagnato da investimenti sistematici in strutture di audit algoritmico indipendente e da programmi di formazione giuridica specializzata capaci di colmare l'asimmetria cognitiva tra regolatori e operatori tecnologici. I principi FAIR, già standard per i dati della ricerca pubblica europea, dovrebbero essere estesi, con opportuni adattamenti, ai sistemi decisionali automatizzati ad alto rischio. La supervisione umana strutturata nel ciclo HAIMLA e la tracciabilità garantita dall'isomorfismo tra norma e rappresentazione algoritmica non sono vincoli tecnici aggiuntivi, ma la forma procedurale che il costituzionalismo digitale assume nell'architettura concreta dei sistemi.

Rimane una tensione che questo lavoro non pretende di risolvere, ma che ritiene necessario nominare con onestà. Il nodo irrisolto resta quello della capacità istituzionale. Governare sistemi che operano a velocità e scale incommensurabili con i tempi della produzione giuridica democratica richiede attori normativi capaci di esercitare una volontà coerente su processi che, per loro natura, tendono a sottrarsi a qualsiasi cristallizzazione regolativa. Il diritto costituzionale lavora sulla durata, sull'accumulazione di precedenti, sulla sedimentazione di valori condivisi; i sistemi di apprendimento automatico evolvono in cicli di aggiornamento continuo che possono rendere obsoleta qualsiasi certificazione di conformità nel giro di mesi. Questa asimmetria temporale tra norma e tecnologia non è risolvibile mediante un incremento quantitativo di regolazione, ma richiede una riprogettazione delle forme stesse della produzione normativa, verso modelli in cui la revisione dei parametri algoritmici sia strutturalmente incorporata nel ciclo legislativo, e non affidata alla reattività contingente del legislatore di fronte agli eventi⁹⁴.

Non è una resa. È il riconoscimento che la governance algoritmica responsabile non è un traguardo compiuto, ma un processo permanente e conflittuale, e che proprio in questo la sua natura si rivela profondamente politica. Le proposte qui avanzate non sono soluzioni definitive, ma rendono visibile ciò che altrimenti resterebbe opaco e creano le condizioni affinché la critica giuridica, politica e sociale possa esercitarsi in modo informato. Resta, alla fine, una scommessa sul soggetto. Il costituzionalismo digitale ha

⁹³ S. RODOTÀ, *Il diritto di avere diritti*, cit.; O. POLLICINO, *Costituzionalismo digitale*, cit.

⁹⁴ L. FLORIDI, J. COWLS, M. BELTRAMETTI *et al.*, *AI4People — An Ethical Framework for a Good AI Society*, in *Minds and Machines*, 28(4), 2018, 689-707; OCSE, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449, Parigi, 2019, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (last visited 23/06/2026).



senso soltanto se esistono, o se si è disposti a costruire, cittadini capaci di interrogare i sistemi che li governano, istituzioni disposte a essere sindacate e giuristi che non rinuncino alla responsabilità di tradurre la complessità tecnica in categorie di giustizia.

*Is
Law*