SFIDE ESISTENZIALI E RESILIENZE IDENTITARIE NELLA GEOPOLITICA INFORMAZIONALE: L'IDENTIKIT EUROPEO TRA SOVRANITÀ E COSTITUZIONALISMO DIGITALE*

di Isabella de Vivo**

Sommario. 1. Introduzione: la *data sovereignty* dalla prospettiva europea. – 2. Datificazione e diritti fondamentali: l'ontologia dei *big data*. – 2.1. il perimetro di tutela del «diritto all' identità personale» secondo il *GDPR*. – 3. La valenza duale dei dati: i dati come asset strategico e il «capitalismo politico» statunitense. – 4. Riflessioni conclusive.

1. Introduzione: la data sovereignty dalla prospettiva europea. La capacità di ogni Stato di definire autonomamente il proprio quadro regolamentare concernente l'economia digitale, il potere di controllo sulle infrastrutture strategiche, sicurezza informatica e disinformazione costituiscono l'attuale sfida «esistenziale» che gli ordinamenti democratici si trovano ad affrontare.

Scenari di emergenza quali l'impatto transfrontaliero delle guerre dell'informazione, dalla crisi pandemica al conflitto russo-ucraino, nonché la crescente tensione sino-americana in tema di *data sovereignty* hanno reso improcrastinabile la necessità di convergenze normative a livello europeo, rendendo palese come sovranità informativa e controllo dei dati sia precondizione di resilienza degli istituti democratici.

In questo scenario, la strategia dell'Unione per costruire la c.d. «sovranità digitale europea» rappresenta il tentativo dell'Europa di riaffermare la propria identità normativo-valoriale a livello geopolitico in linea con le sue radici etiche e costituzionali anche nell'ecosistema digitale.

L'espressione «sovranità digitale» utilizzata, per la prima volta, dalla presidente della Commissione Ursula von der Leyen durante il suo discorso sullo stato dell'Unione del 16 settembre 2020[1], si è diffusa e ricorre in una serie di recenti documenti ufficiali dell'UE, di cui alcuni di carattere strategico[2], gli altri connessi agli atti normativi, emanati ed emanandi, che vanno a comporre il *Digital Services Package (DSP),* ossia in nuovo pacchetto regolamentare

---

* *Sottoposto a referaggio*.

** Dottoranda di ricerca in Storia e culture dell'Europa – Università di Roma La Sapienza.

[1]Cfr. U. Von Der Leyen, *State of the Union,* https://ec.europa.eu; cfr. *A Union That Strives For More: My Agenda for Europe (Political Guidelines for the Next European Commission 2*019-2024), ove U. Von Der Leyen sottolinea l'importanza di investire sulla «nostra sovranità tecnologica». Il presidente della Commissione Junker parlava già dal 2018 dell'«ora della sovranità europea». Cfr. Commissione europea, *State of the Union 2018*: *The Hour of European Sovereignty* https:// ec.europa.eu/info/sites/default/files/soteu2018-speech_en_0.pdf

[2] Si veda ad esempio la *Nuova strategia industriale per l'Europa* della Commissione (10 marzo2020), le conclusioni del Consiglio: *Plasmare il futuro digitale dell'Europa* (9 giugno 2020), le raccomandazioni della Commissione per un approccio comune al 5G (18 settembre 2020), le conclusioni del Consiglio sulla sicurezza cibernetica dei dispositivi interconnessi (10 dicembre 2020), le *Priorità legislative dell'UE per il 2021*(18 gennaio 2021), la *Bussola per il digitale 2030: il modello europeo per il decennio digitale* (9 marzo 2021) e da ultimo i documenti connessi ai regolamenti che vanno a comporre il *Digital Services Package* tra cui il *DSA*, il *DMA*, il *DGA*, il *Data Act*, e l'*AI-Act*.

europeo che segna il punto di svolta verso quella che è stata salutata come la nuova e «terza fase di internet»[3]: il c.d. *regulated internet.*

Distanziandosi dai modelli di stampo stato-centrico, tradizionalmente miranti alla «sovranità informativa nazionale»[4] e rinvenibili tanto in regimi autoritari, quanto in democrazie liberali, la strategia europea per il digitale, nasce e si sviluppa, come alternativa alla dicotomia assiale che distingue il modello liberale basato sull'autoregolamentazione dell'industria (c.d. *industry self-regulation)*[5] cifra della c.d. *open internet era*[6] – dai modelli sovranisti tipici di regimi autoritari quali Russia e Cina [7]. Se le rivendicazioni di questi ultimi, hanno, infatti, da sempre riguardato la governance dei protocolli critici di Internet che consentono l'accesso alle informazioni, il

[3] L. Floridi, *The End of an Era: from Self-Regulation to Hard Law for the Digital Industry,* in *Philos. Technol.* 34, 619-622, 2021. In merito ai problemi e alle relative risposte istituzionali che segnano il passaggio dalla *platformized internet* al *regulated internet,* si veda almeno T. Flew, *Regulating Platforms,* Hoboken, New Jersey*,* 2021.

[4] Sui piani di frammentazione e territorializzazione delle reti tipici degli approcci stato-centrici miranti al *c.d. digital sovereignism o digital statism* si veda M. Mueller, *Will the internet fragment? Sovereignty, globalization and cyberspace,* in Polity. 2017; N. Möllers *Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state,* in *Science, Technology & Human Values*, 46 (1), 112-138, 2020. In particolare sulla *Sovereign RuNet* e il tentativo di rinazionalizzazione della rete russa tramite il controllo dei pacchetti di dati in entrata e in uscita dal territorio in modo da isolare la rete russa dal resto del mondo si veda L. Pétiniaud, K. Limonier, M. Bertran *Russia's Pursuit of Digital Sovereignty*, *political, Industrial and Foreign Policy Implications and Limits*, in G. Glasze, A. Cattaruzza, F. Douzet, F. Dammann C. Bômont, M. Braun, D. Danet, A. Desforges, A. Géry, S. Grumbach, P. Hummel, K. Limonier, M. Münßinger, F. Nicolai, L. Pétiniaud, J. Winkler, C. Zanin, *Contested Spatialities of Digital Sovereignty*, 924-928, 2022. In merito si veda anche J. Nocetti, *Contest and conquest: Russia and global internet governance,* in *International Affairs,* 91(1), 111-130, 2015. Sulla tensione sino-americana per la *digital data sovereignity* e il tentativo statunitense di nazionalizzazione del controllo sui dati si veda G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma,* in *Rivista italiana di informatica e diritto*, 4, (1),113-124, 2022. Nell'ambito degli studi di media sciences, si veda S. Couture, S. Toupin, *What does the notion of "sovereignty" mean when referring to the digital?*, in *New Media & Society,* 21, (2), 2305-2322, 2019.

Per la prospettiva geopolitica si veda anche J. Pohle, T. Thiel, *Digital sovereignty,* in *Internet Policy Review*, 9(4), 2020. Rilevando come il significato specifico di sovranità vari in base ai diversi contesti nazionali e agli accordi degli attori, ma anche e soprattutto in base all'idea e al tipo di autodeterminazione che questi attori enfatizzano, gli studi geo-politici mettono in rilievo come nella prospettiva europea, che fa perno sul concetto di sovranità digitale individuale, l'attuale configurazione della trasformazione digitale, diversamente dagli approcci di stampo autoritario, sembra essere problematizzata come una minaccia allo Stato sovrano – nella misura in cui si traduce in una minaccia al soggetto sovrano, in particolare sul punto si veda J. Winkler e F. Dammann, *Digitally Competent – "Digitally Sovereign" – Digitally Civic*: *geopolitics of Subject Formation in the German Context,* in G. Glaze *et al., passim*, 2023. Si veda anche J. Pohle *Digital sovereignty – a new key concept of digital policy in Germany and Europe*, 2020; D. Lambach, *The Territorialization of Cyberspace* in I*nternational Studies Review*, 22(3), 482-506, 2019; L. Floridi, *The fight for digital sovereignty: what it is, and why it matters, especially for the EU,* in *Philosophy and Technology* 33, (3), 369-378, 2020.

[5] C.d. *Industry self regulation*, in merito si veda *infra.*

[6] La vocazione liberale dell'internet delle origini fondata sull'idea per cui *«Life in cyberspace is regulated primarily through the code of cyberspace»* ha collocato il mondo digitale in una dimensione a-giuridica, basata su una autoregolamentazione di tipo esclusivamente tecnico che, da un lato, avrebbe dovuto consentire il superamento dei limiti territoriali su cui si fondano i modelli tradizionali di *government* e, dall'altro, garantire la libertà degli utenti rispetto ai poteri centralizzati. Cfr. L. Lessig, *Code. Version 2.0*, New York, 2006.

[7] Sulle caratteristiche distintive dell'approccio europeo alla sovranità digitale e le sue intersezioni con il costituzionalismo digitale si veda M. Santaniello, il quale rileva come il progetto europeo per la sovranità digitale «pur promuovendo i valori e i principi delle democrazie liberali, si opponga alle istanze isolazioniste con un approccio polifonico, aperto anche ai contributi della società civile» cfr. *Sovranità digitale e diritti fondamentali un modello europeo di Internet governance,* in *Rivista italiana di informatica e diritto* 4, 1 47-5, 2022; id. *La regolazione delle piattaforme e il principio della sovranità digitale*, in *Rivista di Digital Politics*, 3, 579-600, 2021; G. De Gregorio, P. Dunn, *Profiling under Risk-based Regulation: Bringing together the GDPR and the DSA*, in *ctfassets.net*, 2018; S. Torregiani, *Il Data Act: una versione europea del Data Nationalism*?, in *Rivista Italiana di Informatica e Diritto*, 5, 2, 131-146, 2024.

progetto europeo si inserisce e va letto, infatti, nel quadro del «costituzionalismo digitale»[8], ossia quella «costellazione di iniziative che hanno provato ad articolare un insieme di diritti politici, norme di governance, e limitazioni all'esercizio del potere su Internet»[9] volte a ripristinare l' equilibrio costituzionale prodotto dall'avvento della tecnologia digitale. Emerge dunque un'idea di sovranità non quale fine in sé, ma quale obiettivo strumentale e preordinato a dotare di efficacia i principi elaborati nel framework di un costituzionalismo «spontaneo» e ciò tramite il recupero dalla centralità del momento politico (*Political costitutionalism*) - segnatamente, della deliberazione democratica – nella tutela dei diritti fondamentali[10].

In un ecosistema come quello digitale, per vocazione transnazionale, che vede la cesura di quell'accoppiamento strutturale tra diritto e politica che nelle Costituzioni nazionali ha trovato la propria sintesi[11], il costituzionalismo digitale è emerso, infatti, quale forma di «costituzionalismo sociale» *(Societal consitiutionalism*) ossia come espressione di una democratizzazione autopoietica della rete, nata sulla spinta di soggetti che operano al di fuori di un contesto strettamente politico, come le organizzazioni non governative e le comunità epistemiche.[12] Il nuovo *corpus* regolamentare (*Digital Services Package*) espressione dell'attuale approccio europeo all'internet governance, mira, allora, «ad abilitarlo proceduralmente» al fine di rendere effettiva la protezione dei diritti fondamentali al di là dei confini territoriali[13] .

8 Per una rassegna della letteratura sul tema del costituzionalismo digitale si veda E. Celeste, *Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges*, in HIIG *Discussion Paper Series,* 2, 2018 ed in generale sul tema: G. De Gregorio *The rise of digital constitutionalism in the European Union*, in *International Journal of Constitutional Law,* 19, (1), 41-70, 2020; N. Suzor, *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms,* in *GigaNet: Global Internet Governance Academic Network, Annual Symposium* 2016, SSRN: http://dx.doi.org/10.2139/ssrn.2909889. Sui rapporti che intercorrono tra discorso politico e processi di costituzionalizzazione della rete: C. Padovani, M. Santaniello, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Inter-net Eco-System,* in *International Communication Gazette,* 80, 4,.295-301, 2018; M. Santaniello, E. De Blasio, N. Palladino, D. Selva, E. De Nictolis, S. Perna, *Mapping the debate on Internet Constitution in the networked public sphere,* in *Comunicazione politica,* 3, 327-35, 2016.

9 Così L. Gill, D. Redeker, U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, *Berkman Center Research Publication*, 15, 2015, 2.

10 Sul concetto le diverse declinazioni e i relativi limiti del costituzionalismo politico si veda G. Pino, *Chi deve essere il custode dei diritti?* in *Rivista di Diritti comparati,* 3, 1, 2022; nella dottrina internazionale in tema di *political constitutionalism*: J. Waldron, *A Right-Based Critique of Constitutional Rights,* in *Oxford Journal of Legal Studies,* 13, 1,18-51, 1993; T. Campbell, *Prescriptive Legal Positivism. Law, Rights and Democracy,* London, 2004. Con riferimento alla dottrina italiana A. Pintore, *Diritti insaziabili, in L. Ferrajoli, Diritti fondamentali. Un dibattito teorico,* E. Vitale, (a cura di), Roma-Bari, 2001, 9-200*; id., I diritti della democrazia,* Roma-Bari, 2003.

11 Cfr. G. Teubner, *Global Bukovina. Legal pluralism in the World Society,* in G. Teubner (ed.), *Global law without a State,* Aldershot, 1997, 6.

12 Si rimanda ancora a G. Teubner*, Societal Constitutionalism; Alternatives to State-Centred Constitutional Theory?*' in C. Joerges, I.J. Sand, G. Teubner (a cura di), *Transnational Governance and Constitutionalism. International Studies in the Theory of Private Law*, Hart 2004; Id. *Constitutional Fragments: Societal Constitutionalism and Globalization,* Oxford, 2012; id. *The project of constitutional sociology: Irritating nation state constitutionalism,* in *Transnational Legal Theory,* 4, 44-58, 2013; Id. *Nuovi conflitti costituzionali,* Milano, 2012, 69; Id. *Il costituzionalismo della società transnazionale, in Quaderni costituzionali,* 1, 2014, 196; A. JR. Golia, G. Teubner, *Societal Constitutionalism: Background, Theory, Debates*, in *ICL Journal,* 15, 4, 357-411, 2021. Per una visione critica si veda M. Betzu, *I poteri privati nella società digitale:* in *Diritto pubblico*, 3, 2021.

13. Cfr. M. Santaniello, *Sovranità digitale e diritti fondamentali*, *passim*, 49, il quale descrive una «maturazione» del costituzionalismo digitale, che non si limita più a una mera elencazione di diritti e principi, ma si spinge fino a costruire, e a organizzare, un nuovo insieme di poteri pubblici, il cui esercizio è posto in capo a vecchie e nuove istituzioni. Così anche E. Celeste, *Digital Sovereignty in the EU: Challenges and Future Perspectives.* in F. Fabbrini, E. Celeste, J. Quinn (a cura di), *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart, 2021. Il modello europeo rappresenterebbe, dunque, un tentativo di democratizzare e costituzionalizzare Internet cfr. G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union* 19(1) in *International Journal of Constitutional Law,* 41-70, 2020

Vi è tuttavia un *discrimen* importante rispetto alle forme di costituzionalismo pre-digitale: se quest'ultime hanno, infatti, storicamente affrontato e limitato l'esercizio del potere da parte dello Stato nazionale e l'autonomia dei privati è stata costruita in un'ottica di bilanciamento con il potere pubblico, nel mondo digitale sono le grandi piattaforme a interfacciarsi con le persone, raccogliendone i dati, profilandole, condizionandone il pensiero. Nel mutato contesto geopolitico lo sforzo è, dunque, prima di tutto volto ad arginare il potere politico di attori che potremmo definire «ibridi»[14] o «para-pubblici»[15] in grado di limitare prerogative tipicamente statuali quali il bilanciamento dei diritti fondamentali.

Assumendo configurazioni sempre più simili allo Stato e ad altre autorità pubbliche, la loro struttura sembra riflettere un cambiamento fondamentale nei sistemi politici e giuridici delle democrazie occidentali, seguendo la direttrice di quello che è stato definito un nuovo tipo di «sovranità privata funzionale»[16]. Il costituzionalismo digitale consiste, allora, primariamente nell'articolare i limiti dell'esercizio del potere privato della società in rete[17] in modo da sfidare l'emergente «algocrazia»[18].

Data la vocazione naturalmente transnazionale della governance del digitale, il cambiamento paradigmatico che caratterizza il mutato contesto geopolitico è, tuttavia, duplice. Le forme di colonialismo normativo/culturale derivanti dall'imposizione surrettizia di assetti valoriali e obiettivi strategici non sempre compatibili con le prerogative dell'Unione, derivano non soltanto dalla «privatizzazione»[19] del bilanciamento dei diritti fondamentali, ma anche dalle interferenze governative extra-UE che vedono poteri pubblici e privati- «uniti per la sorveglianza»[20] - porsi in rotta di collisione con gli standard di tutela che informano l'architettura costituzionale europea. In conseguenza, le sfide poste dal nuovo ordinamento algoritmico (o meglio algocratico) e la sua costante evoluzione, coinvolgono ampiamente il

---

14 Sul tema la letteratura è amplissima si veda almeno: G. De Gregorio, *The Law of the Platforms. In: Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society,* in *Cambridge Studies in European Law and Policy,* Cambridge, 80-122, 2022; M. Bassini, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *Rivista italiana di informatica e diritto,* 2, 43-64, 2021; O. Pollicino, G. De Gregorio *Constitutional Law in the Algorithmic Society*, passim; A. Simoncini, E. Longo, *New technologies and the rise of the algorithmic society*, in H-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (a cura di). *Constitutional Challenges in the Algorithmic Society,* Cambridge, 3,24, 1-23, 2021; A. Venanzoni, *Cyber-costituzionalismo: la società digitale, passim,* 5-34.

15 Parla di funzione «quasi-pubbliche» G. De Gregorio, *From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society,* in *European Journal of Legal Studies,* 11(2), 65-103, 2019, 3; id. *The rise of digital constitutionalism*, *passim*, 18 e ss. O. Pollicino, *Google rischia di «vestire» un ruolo para-costituzionale*,in Il Sole 24 Ore, 14 maggio 2014.

16 F. Pasquale, *From-Territorial-To-Functional-Sovereignty. The Case Of Amazon*, in *opendemocracy.net,* 2018; D. Feldner, *Designing A Future Europe,* in D. Feldner (a cura di), *Redesigning Organizations: Concepts for the Connected Society*, 2020.

17 Così C. Padovani, M. Santaniello, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System, passim*, 295-301.

18 Cfr. J. Danaher, *The Threat of Algocracy: Reality, Resistance and Accommodation,* in *Philosophy and Technology* 29 (3), 245-268, 2016.

19 Si veda in merito M. Bassini, *Internet e libertà di espressione. Prospettive costituzionali e sovranazionali*, Roma, 2019. Sull'attività del *FB Oversight Board* come plastica espressione della «privatizzazione della giustizia digitale su scala globale» si veda O. Pollicino, L' "*autunno caldo" della Corte di giustizia in tema di tutela dei diritti fondamentali in rete e le sfide del costituzionalismo alle prese con i nuovi poteri privati in ambito digitale*, in *Federalismi.it*, 19, 2019.

20 In merito si veda Simitis, il quale rileva come il governo americano «non si attenga più alla tradizionale raccolta diretta di dati, ma si rivolga a entità private. Così facendo, lo Stato non solo riconosce che la maggior parte dei dati è conservata nel settore privato, ma stabilisce anche un modello di elaborazione che combina sistematicamente le informazioni raccolte sia nel settore pubblico che in quello privato». S. Simitis, *Privacy - An Endless Debate?* In *California Law Review*. 98,1989-2005, 2010, 2003. Sulle «porte girevoli» tra *Google* e il Governo americano si veda S. Zuboff, *The Age of Surveillance Capitalism, The fight for a human future at the new frontier of power,* 122, New York, 2019.

principio dello Stato di diritto non soltanto per la questione relativa ai limiti da imporre alla determinazione privata nell'implementazione di tali tecnologie a protezione dei diritti fondamentali, ma anche in relazione alla possibilità di assicurare a livello tanto transnazionale, e come vedremo anche regionale, gli standard di protezione garantiti a livello europeo.
In questa nuova architettura verticalmente triangolare e orizzontalmente globale che informa l'economia digitale, il tema della governance e del controllo di quella che ne costituisce la risorsa base – i c.d. *big data* – è necessariamente trasversale a qualsiasi tentativo di regolazione della rete e vede dunque convergere al suo interno gli attuali sforzi normativi dell'UE (dal GDPR al lancio da parte della Commissione della Strategia per il Mercato Unico dei Dati, al *Digital Services Package*) che descrivono l'attuale metamorfosi della governance della rete.
Nel tentativo di comprendere appieno gli obiettivi e gli ostacoli che, a livello internazionale e regionale, attualmente, si frappongono al descritto tentativo europeo di costituzionalizzazione del digitale, attraverso il primario obiettivo di garantire una data governance globale orientata alla tutela dei diritti fondamentali, con l'analisi che segue si proverà, preliminarmente, a disambiguare la comprensione della natura dei dati - comunemente definiti la «nuova materia prima» del «capitalismo informazionale» (o *plaform capitalism*)[21] – mettendone in luce la natura essenzialmente bifronte derivante dalla loro rilevanza strategica tanto nel settore civile, quanto militare.
Per quanto, infatti, le operazioni di sorveglianza e di *data mining*[22] vengano, solitamente intese da un punto di vista strettamente commerciale, motivo per cui per cui la maggior parte degli studi e delle ricerche tende a concentrarsi in particolare sull'analisi dei dati estratti dalle grandi

[21] Il termine «capitalismo di piattaforma», anche detto «capitalismo informazionale» o «capitalismo dei big data», vede un ristretto oligopolio di società private, (il riferimento va in particolare all'oligopolio pentagonale costituito dalla c.d. GAFAM: Google, Apple, Facebook, Amazon, Microsoft negli USA e alla c.d. BATX: (Baidu, Alibaba, Tencent, Xiaomi, in Cina), detenere il controllo della maggior parte delle infrastrutture critiche e del relativo traffico dati, condizione da cui deriva l'accentramento del controllo delle condizioni di esistenza e possibilità dell'intero spazio comunicativo globale nonchè le stesse possibilità di esistenza dello spazio. Sul tema e per la definizione di capitalismo informazionale si veda J. Cohen, *Between Truth and Power: the Legal Constructions of Informational Capitalism,* Oxford 2019; C. Fuchs *Karl Marx in the Age of Big Data Capitalism. Digital Objects*, in: D. Chandler, C. Fuchs (a cura di) *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics, in the Age of Big Data*, London, 2019. Si veda altresì N. Srincek, *Platform capitalism.* Polity Press, tr.it. a cura di C. Papaccio, *Capitalismo digitale,* Roma, 2017; N. Couldry, U.A. Meijas,*The costs of connection: How data is colonising human life and appropriating it for capitalism*. Stanford, 2019; D.Nguyen, B. Beijnon, *The data subject and the myth of the 'black box' data communication and critical data literacy as a resistant practice to platform exploitation*, in *Information, Communication & Society,* 2023.

[22] *Il data mining* è il processo di esplorazione e analisi di enormi volumi di dati detenuti da grandi organizzazioni, governi e colossi tecnologici per scoprire *pattern* nascosti, relazioni all'interno dei dati, trend e altre informazioni significative. Set provenienti da diverse fonti (come database, *data warehouse*, file di log, social media e sensori) vengono analizzati ed animati strutturando ed estraendo conoscenza e valore da tracce digitali eterogenee, tramite tecniche di *big data analytics*, *machine learning* – basato tanto su algoritmi di apprendimento supervisionato (es. alberi decisionali, reti neurali), quanto su algoritmi di apprendimento non supervisionato (es. *k-means clustering,* algoritmi di associazione) – e *deep learning* (reti neurali artificiali). Volendo fornire un quadro orientativo dei principali settori in cui il *data mining* trova applicazione, comunemente oggetto di indagine, avremo: 1) *Marketing:* analisi del comportamento per segmentare il mercato e personalizzare le offerte; previsione delle vendite e analisi delle tendenze di mercato; 2) Comunicazione, *Social Media*: analisi dei sentimenti, monitoraggio delle tendenze; determinazione dei comportamenti di consumo informativo tramite algoritmi di raccomandazione (RS) e di personalizzazione dei contenuti; 3) Finanza: rilevamento di frodi finanziarie e gestione del rischio; analisi del credito e previsione delle insolvenze; 4) Sanità: analisi dei dati dei pazienti per migliorare la diagnosi e il trattamento; monitoraggio delle epidemie e gestione della salute pubblica; 5) Produzione e Logistica: ottimizzazione dei processi produttivi e gestione della catena di approvvigionamento. Come vedremo, tuttavia, il settore civile non esaurisce l'ambito di sviluppo e applicazione delle tecniche di data mining.

piattaforme a scopo pubblicitario[23], non può dimenticarsi come i dati, presupposto ontologico dello sviluppo dell'Intelligenza Artificiale – costituiscano al contempo, la *condicio sine qua non* della implementazione della stessa anche in campo bellico. Si proverà, dunque, preliminarmente, ad affrontare tale questione attraverso una più ampia riflessione circa l'impatto strutturale della datificazione – *core business* delle piattaforme digitali – sulla garanzia dei diritti sanciti dalla Carta europea dei diritti fondamentali e in particolare sul principio dell'identità personale; con la seconda parte del lavoro, concentreremo l'analisi sull'ulteriore e menzionato aspetto, destinato ad incidere sul disegno europeo di data-governance globale, ossia la valenza strategica dei *big data* nel settore militare, mettendo in luce come raccolta pervasiva di dati, stia trasformando le vulnerabilità individuali e commerciali anche in potenziali debolezze inerenti alla sicurezza nazionale.

Nell'attuale geopolitica del capitalismo informazionale[24], come si avrà modo di approfondire nel prosieguo della trattazione, i dati raccolti su un determinato territorio, o meglio dalle popolazioni che lo abitano, sono in grado di incidere su sicurezza e resilienza delle società democratiche, non soltanto indirettamente, attraverso l'interferenza sul corretto funzionamento degli istituti democratici (si pensi ai processi di formazione dell'opinione pubblica e della volontà elettorale), ma anche direttamente, rappresentando a tutti gli effetti una minaccia in termini di sicurezza e autonomia geopolitica degli Stati nazionali in quanto *asset* strategico per lo sviluppo dell'IA anche in campo bellico. Una circostanza che, chiamando in causa le prerogative statali legate alle ragioni di sicurezza, non può che riflettersi sul perimetro e sull'efficacia della regolazione sovranazionale a livello tanto regionale, quanto globale. È con tale intrinseca valenza duale dei dati, che la sovranità digitale europea e l'«autonomia strategica»[25] che essa presuppone, ossia la generale capacità di salvaguardare gli interessi e i valori di cui si fa portatrice, è chiamata a confrontarsi.

2. Datificazione e diritti fondamentali: l'ontologia dei big data. Premessa fondamentale, di un progetto politico sovranazionale che si vuole antisovranista[26], mirante ad un approccio polifonico ed aperto, dovrebbe essere quella di garantire le condizioni per pensare uno spazio che possa essere definito come una «sfera pubblica digitale europea» o, meglio, come una sfera pubblica transnazionale[27]. In assetti costituzionali, come quelli che caratterizzano il panorama europeo, imperniati sulla centralità dell'individuo, e sul compito dello Stato di rimuovere gli ostacoli che impediscono il pieno sviluppo della personalità del singolo, la pervasiva capacità dei sistemi di IA di «datificare» le esistenze individuali, erodendo le possibilità decisionali dell'individuo attraverso un costante e spesso oscuro processo di ridimensionamento dell'opportunità di conoscenza e delle alternative di scelta, costituisce oggi un pericoloso *vulnus* nel percorso evolutivo tali società, minando dalle fondamenta i

[23] In merito si veda A. Aresu, *Lo Stato nella competizione tecnologica,* in *Rivista trimestrale di cultura e di politica,* 2, 84-92, 2023.

[24] Sulla definizione del concetto si veda *supra*, nota 21.

[25] Cfr. *Una strategia globale per la politica estera e di sicurezza dell'Unione europea*, 28 giugno 2016, http://europa.eu/globalstrategy/en.

L'autonomia strategica è concepita come strumento per affrontare minacce complesse: da qui la declinazione del concetto sotto il profilo della cd. sovranità tecnologica, digitale, energetica, industriale, alimentare, economica dell'UE, perseguita dalla Commissione europea con vari strumenti e a vari livelli, al fine di coinvolgere nel processo di trasformazione strategica gran parte delle politiche dell'Unione. Sul tema si veda M.E. Bartoloni, *La politica di sicurezza e di difesa comune dell'UE: verso un'"autonomia strategica" o "strategie in autonomia"*?, in *Le Istituzioni del Federalismo*, 1, (2), 45-64, 2022; S. Poli, E. Fahey, *The strengthening of the European technological sovereignty and its legal bases in the Treaties*, in *Rivista.eurojus.it,* 2022.

[26] Cfr. M. Santaniello, *Sovranità digitale e diritti fondamentali, passim,* 50.

[27] P. Schlesinger, *After the post-public sphere,* in *Media, Culture & Society,* 42, (7–8), 1545 15-63, 2020.

presupposti non solo del dibattito democratico, ma finendo per interferire indebitamente nell'esercizio di diritti che attengono agli attributi ontologici della persona. Se democrazia e tutela dei diritti fondamentali, *in primis* il «diritto all'identità personale» che il libero agire presuppone[28], sono indissolubilmente legati, l'impatto e la pervasività della raccolta dati e dell'analisi algoritmica - presentano sfide inedite al diritto costituzionale. Comprendere che genere di risorsa siano «i dati» su cui gli algoritmi operano, è, dunque, premessa indispensabile non soltanto per individuare la rilevanza dei diritti in gioco, ma anche per inquadrare il contesto geopolitico entro cui si gioca la sfida europea per la costruzione di una *data governance* coerente con il proprio assetto valoriale.

Il primo punto che necessita, allora, di disambiguazione riguarda il genere di risorsa che si è soliti intendere alla base del *big data capitalism*[29], in modo da inquadrare gli interessi ed i diritti coinvolti e, dunque, il frame teorico-normativo di riferimento.

La narrativa prevalente porta a concepire i dati, in particolare i *raw data* (dati grezzi), come «materia prima» della *data economy* intendendoli, dunque, al pari di ogni altra risorsa naturale, come preesistenti a qualsiasi attività umana e pertanto liberamente disponibile all'appropriazione. Emblematica al riguardo è la dichiarazione di Schmidt del 2017, ex CEO di Google ed allora presidente del *Defence Innovation Board* (DIB)[30]resa durante la quinta sessione pubblica dell'Organo, secondo cui «I dati [sarebbero] l'equivalente del 21° secolo di una risorsa naturale globale, come il legname, il ferro o il petrolio[…]»[31].

Una narrazione questa che, tuttavia, oltre ad essere epistemologicamente fuorviante, rischia di oscurare i presupposti ideologici alla base della quantificazione del sociale. Contrariamente al suo etimo, il dato come *datum*, liberamente disponibile in natura, non esiste, trattandosi invece del risultato di un processo, storicamente e socialmente situato, di co-costruzione, ri-definizione e successiva appropriazione[32]. Parlare di «materia prima» prodotta astraendo e riducendo il mondo in forme rappresentative e definirla *raw data* significa sostenere un - ossimoro[33].

---

[28] Per un'ampia trattazione del concetto di «privacy informazionale» basata sull'isomorfia tra flussi di dati e flussi esistenziali si veda L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo,* Milano, 2017. Sulla necessità di riformulare il diritto alla privacy come il diritto all'identità personale, ovvero alla libertà di costruzione (o co-costruzione) e sviluppo autoriale del proprio progetto identitario, si veda: E.M. Renieris, *Beyond data: reclaiming human rights at the dawn of the metaverse*, Cambridge, 2023; S.O. Søe., J.E. Mai, *Data identity: privacy and the construction of self. Synthese*, 200(6), 492, 2022; C. Koopman, *How we became our data: A genealogy of the informational person*. Chicago, 2019; da ultimo S. Tiribelli, *Identità personale e algoritmi, Una questione di filosofia morale*, Roma. 2023.

[29] Si veda *supra* nota 21.

[30] Il *Defense Innovation Board,* istituito nel 2016, è un organo consultivo indipendente creato per portare l'innovazione tecnologica e le migliori prassi della Silicon Valley all'esercito degli Stati Uniti e al Dipartimento della Difesa (DoD). Il Consiglio, regolamentato dal F*ederal Advisory Committee Act* (FACA), offre raccomandazioni indipendenti al Segretario della Difesa e comprende esperti da settori commerciali, ricerca e accademia. Il Consiglio è stato fondato per portare le migliori pratiche innovative in termini di tecnologia, forza lavoro e struttura organizzativa al Dipartimento della Difesa. Dal 2016 è impegnato nella ricerca di idee innovative provenienti dai soggetti coinvolti nelle operazioni militari per migliorare i processi utilizzati nei teatri operativi a livello globale. Joshua Marcuse e il Dr. Eric Schmidt sono stati rispettivamente il primo Direttore Esecutivo e il primo Presidente del Consiglio. L'organizzazione svolge un ruolo fondamentale per il Dipartimento della Difesa, nella consulenza per l'innovazione strategica in aree chiave quali appunto l'Intelligenza Artificiale.

[31] Cfr. Verbale della *Defense Innovation Board* - 24 ottobre 2017 e *Recommendation* 12: *Forge New Approach to Data Collection, Sharing, and Analysis* https://innovation.defense.gov/Portals.

[32] Cfr. R. Kitchin, *Thinking critically about and researching algorithms.* in *Information, Communication* & Society, 20,1-16, 2019; L. Gitelman, *Raw Data is an Oxymoron,* Cambridge, 2013.

[33] L. Gitelman, *Raw Data is an Oxymoron,* 2013, *passim;* R. Kitchin, *Thinking critically about and researching algorithms,* 2019, *passim.*

L' espansione degli orizzonti merceologici del capitalismo informazionale avviene, infatti, tramite la mercificazione di una risorsa sicuramente nuova, in quanto fino adesso estranea alle logiche estrattive, ma di cui i dati rappresentano soltanto il prodotto; a costituire la materia prima alla base della *data economy* sono infatti le relazioni umane in quanto tali che, codificate sottoforma di *data relations*[34], sono strutturate per la mercificazione sul mercato primario e secondario dei dati. Oggetto di «propiziazione»[35] è, dunque, l'esistenza umana in quanto tale che, trasposta in ogni singolo aspetto individuale e relazionale nella dimensione dell'*onlife*[36], si fa materia prima di quel processo – interpretativo e costitutivo – che è l'estrazione algoritmica della conoscenza[37].

Se il *data mining*, strumentale all'economia dell'attenzione, agisce sul principio di autodeterminazione individuale, estraendo valore non soltanto dalla previsione, ma anche dalla direzione del pensiero e dell'azione, rendendo possibile la conoscenza profonda e capillare dell'individuo, delle sue attitudini, orientamenti, valori e comportamenti [38], è chiaro che quando si tratta di raccolta dati e della sua governance a venire in discussione è la protezione del nucleo essenziale dei diritti individuali su cui le tradizioni costituzionali europee fondano la propria identità. In conseguenza, come si argomenterà nel corso della trattazione, parlando di «*privacy* informazionale»[39] non è alla tutela della riservatezza in senso analogico del termine a cui deve farsi riferimento, ma a quello spazio identitario minimo – di cui è la «libertà epistemica»[40] è presupposto ontologico – a garanzia di uno sviluppo che possa dirsi moralmente libero della personalità individuale [41]. In altre parole, in gioco è la tutela dell'auto-sovranità cognitiva che l'agire libero presuppone e da cui, a sua volta, dipende la resilienza di una sfera pubblica e di un corpo elettorale autonomi, condizioni indefettibili della legittimità della «sovranità dei poteri»[42]. L'idea stessa di «sovranità dei poteri», soggettivamente intesa, ha senso, infatti, se ed in quanto la si intenda in funzione servente

[34] Cfr. N. Couldry, U.A. Meijas, *The costs of connection: How data is colonising human life and appropriating it for capitalism*.,2019, *passim.*

[35] Il termine propiziazione, letteralmente riferito a pratiche rituali è efficacemente utilizzato da, Couldry e Mejias quale metafora per descrivere come le dinamiche di stampo colonialistico di estrazione dei dati, creino le condizioni strutturali favorevoli, o meglio propizie, a determinate configurazioni di potere e controllo sociale. Cfr. N. Couldry, U.A. Meijas, *The costs of connection: How data is colonising human life and appropriating it for capitalism*., 2019, *passim.*

[36] Cfr. L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo* 2017, *passim.*

[37] Sulle tecniche di *data-mining* si veda *supra,* nota 22; Sul tema si veda ancora L. Gitelman, *Raw Data is an Oxymoron,* 2013, *passim.;* D. Beer, *The Social Power of Algorithms,* in *Information,* in *Communication & Society*, 20, 1, 1-13, 2017.

[38] La c.d. economia dell'attenzione trae il suo vantaggio economico attraverso l'accentramento dell'unica risorsa che può dirsi «scarsa» nel panorama dell'*overload* informativo ossia l'attenzione degli utenti, dal cui «impossessamento» deriva il vantaggio competitivo per aziende e intermediari.

[39] Sulla concettualizzazione e le declinazioni della privacy c.d. informazionale si veda *supra* nota 28.

[40] Ossia la libera determinazione dei propri orizzonti cognitivi: per una più ampia trattazione riguardo la natura multidimensionale dell'identità, sia consentito rimandare a I. de Vivo, *Il sé allo specchio dell'algoritmo, libertà epistemica e identità individuale,* 55-74 in A. Sterpa, (a cura di) *L'ordine giuridico dell'algoritmo,* Napoli 2023.

[41] È implicito in quest'impostazione il riconoscimento del legame costitutivo tra identità personale e libertà cognitiva, e quindi l'idea che per cui almeno in parte, le nostre identità e le nostre vite sono plasmate dalle scelte che compiamo. Sull'impatto delle tecnologie algoritmiche sulla dimensione etica nella costruzione dell'identità personale e quindi sulla libertà morale che essa sottende, si veda S. Tiribelli, *Identità personale e algoritmi, una questione di filosofia morale*, Roma 2023, *passim,* 15.

[42] La partecipazione politica, sia in forma attiva che in forma passiva, presuppone il possesso di un bagaglio informativo da parte del cittadino-elettore affinché possa criticamente formare la propria opinione orientando la propria scelta, così come postula che il cittadino-candidato non incontri ostacoli nell'esercizio della libertà di parola.

della «sovranità dei valori»[43] che appunta la sua ragion d'essere nel riconoscimento dei diritti fondamentali, quale «cuore pulsante e giustificazione della sua esistenza»[44].
A livello fenomenico, l'«incorporazione» biunivoca tra determinazione umana e algoritmica attraverso la datificazione, può avvenire non soltanto attraverso la «delega diretta» ed esplicita della decisione/valutazione al sistema automatizzato, ma anche attraverso una «delega indiretta», forse meno visibile, ma non per questo meno rilevante, che attiene il momento che della determinazione volontaristica è il presupposto[45]. Gli algoritmi e i dati, anche quando non direttamente chiamati in causa, come nel caso della moderazione automatizzata dell'informazione operata dalle piattaforme digitali su scala globale, forniscono il terreno culturale e cognitivo e finanche la prospettiva morale, in base a cui gli agenti umani formano opinioni e prendono decisioni, in altre parole, esercitano quei diritti che definiscono la libertà di espressione nella sua accezione più ampia del termine. Libertà negativa per eccellenza, la libertà di espressione, come noto, trova al tempo stesso nel suo risvolto positivo -il diritto al pluralismo informativo, alla trasparenza nelle opzioni di scelta e alla qualità delle fonti informative- il suo presupposto indefettibile. Spingendoci ancora oltre nell'analisi, quella che definiamo «libertà epistemica» è, infatti, la condizione imprescindibile perché possa ipotizzarsi un diritto alla «libertà morale», ossia quel «diritto a determinarsi liberamente nella scelta dei propri percorsi esistenziali […] e che consente alla persona di avere specifica percezione del sé quale soggetto responsabile e non mero oggetto passivo della propria esperienza esistenziale»[46].
Shock pubblici, come le conseguenze dello scandalo *Cambridge Analytica* del 2018[47], hanno,

[43] Il riferimento è ad una nota indicazione teorica di G. Silvestri, *Lo Stato senza principe. La sovranità dei valori nelle democrazie pluraliste*, Torino, 2005.
[44] Così A. Ruggeri, *Sovranità e autonomia regionale, dal modello costituzionale al tempo dell'emergenza (prime notazioni)*, in *Saggi* 1-2021, 123. https://*www.nuoveautonomie.it*
[45] In questi termini, riferendosi ad un doppio regime di «mutazione del mezzo tecnico» in relazione alla natura diretta o meno della sua incorporazione nel processo decisionale umano, si veda A. Simoncini, S. Suweis*, Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale,* in *Rivista di filosofia del diritto, Journal of Legal Philosophy*, 87-106, 1, 2019, 94.
[46] Con queste parole si è espressa la Cassazione in merito ad una fattispecie seppur diversa, collegata e di estrema rilevanza per il profilo oggetto di trattazione, ossia il colpevole ritardo diagnostico. L'omissione o il ritardo informativo in questo caso, secondo il giudice di legittimità, integrerebbe un'autonoma lesione apprezzabile sul piano sostanziale, indipendentemente all'esito della patologia (nel caso al vaglio della Corte certamente infausto) e dal danno derivante dall'eventuale perdita di *chances*, consistente «nella violazione del diritto del paziente a determinarsi liberamente nella scelta dei propri percorsi esistenziali […] situazione soggettiva di libertà- immediatamente riconducibile al valore supremo della dignità». Cfr. Cass. civ., sez. III, ord. 23 marzo 2018, n. 7260.
[47] Il caso *Cambridge Analytica*, scoppiato nel 2018, è stato uno dei più grandi scandali relativo a privacy e manipolazione dei dati nella storia recente. La società britannica di consulenza politica e analisi dei dati, è stata infatti accusata di aver prelevato enormi quantità di dati (87 milioni di profili Facebook) di utenti del tutto ignari, influenzando, attraverso tecniche di profilazione psicografica e di *hypernudging* (su cui si veda nota *infra),* la campagna elettorale presidenziale statunitense del 2016, nonché l'esito del referendum *Brexit.* La società avrebbe, infatti, lavorato al fianco della campagna elettorale di Donald Trump nel 2016 e dei sostenitori della Brexit, fornendo loro gli strumenti per il *micro-targeting* elettorale. In conseguenza della risonanza pubblica dello scandalo e della sanzioni inflitte a Facebook (di 5 miliardi di dollari è la multa della *Federal Trade Commission* (*FTC*) degli Stati Uniti e di 500,000 sterline quella comminata dall' *Information Commissioner's Office* (*ICO*) del Regno Unito, che ha previsto l'importo massimo possibile secondo la legge britannica vigente all'epoca), la piattaforma ha intrapreso una serie di significative (seppur discutibili) riforme interne volte a migliorare la sicurezza dei dati e la trasparenza. Tra queste vi è l'istituzione di un Consiglio di Supervisione indipendente *(FB Oversight Board)* con funzioni para-giudiziali a garanzia della trasparenza delle politiche di moderazione adottate dalla piattaforma stessa. Sulle preoccupazioni relative alla privacy e alla tutela dei diritti fondamentali a seguito dello scandalo da parte delle istituzioni europee ed il conseguente cambio di marcia della strategia in materia

del resto, reso noti i pericoli insiti nella capacità di elaborazione dei dati per la tutela dei diritti fondamentali palesando l'esposizione individuale alla sorveglianza a scopi predittivi (*data-veillance*[48]) e alla manipolazione informazionale intenzionale[49] (profilazione psicografica e di *hypernudging*[50]) e le sue dirette conseguenze sul corretto funzionamento dei processi elettorali. Il drammatico impatto dei descritti fenomeni distorsivi, e il conseguente *techlash* globale[51], non poteva non dare nuovo impulso al dibattito circa la natura degli interventi normativi necessari ed idonei a controbilanciare l'opacità delle forme ibride di controllo sui flussi informativi, basate sul *data mining* algoritmico. È in questa direzione che si muove il citato *Digital Services Package* ed in particolare *il Digital Services Act* (*DSA*)[52], il regolamento europeo che, per la prima volta, interviene nell'oligopolio informativo digitale, dettando una disciplina coercitiva *ex ante,* generale e orizzontale, in tema di *content moderation* e *content curation*, direttamente esecutiva per piattaforme e Stati Membri. Con l'emendamento del c.d. principio del *safe harbor*[53] (cfr. dir. UE 2000/31) – corollario del regime transnazionale di *industry self-regulation* che a partire dagli anni Novanta ha caratterizzato, per lo più senza soluzioni di continuità, la governance della rete negli Stati liberali – e dunque con il riconoscimento della responsabilità giuridica delle piattaforme digitali in relazione ai contenuti illeciti e/o dannosi diffusi per loro tramite, l'obiettivo dichiaratamente perseguito per i casi di mancata rimozione dei contenuti segnalati come illeciti e/o dannosi è quello di garantire uno spazio digitale transnazionale in cui i diritti fondamentali siano protetti. Nonostante il lodevole intento, e prescindendo in questa sede dai problemi relativi alla formalizzazione *ex lege* della delega sostanziale[54] alle piattaforme di prerogative storicamente di appannaggio pubblico, quali la

governance dei dati si veda: T. Madiega, *Digital sovereignty for Europe,* EPRS, 2020, https://www.europarl.europa.eu/

48 Cfr. D. Lyon, *Surveillance culture, ethics and digital citizenship.* in *International Journal of Communication,* 11, 824 - 842, 2017.

49 Si veda almeno D. Beer, *The Social Power of Algorithms,* in *Information*, 2017, *passim;* L. Gitelman, *Raw Data is an Oxymoron,* 2013 *passim.*

50 Si tratta di quelle strategie che impostano il contesto della scelta delle informazioni da parte dell'utente in modo intenzionalmente progettato per manipolare le sue decisioni, cfr. K. Yeung, *"Hypernudge": big data as a mode of regulation by design,* in *Inf. Commun. Soc.* 20 (1), 118-136, 2018. L'ambiente algoritmico, di fatto, si modella costantemente attorno al soggetto e alle tracce della sua biografia digitale; è mimetico e presenta certamente diverse analogie con il *nudging* che, come pratica di regolazione comportamentale, non riguarda la creazione e l'interiorizzazione di valori e norme, ma si fonda sulla costruzione di particolari architetture di scelta e di comportamento che circoscrivono le possibilità di azione degli attori sociali.

51 B. Zimmer, *Techlash: Whipping Up Criticism of the Top Tech Companies',* in *Re Wall Street Journal*, 2019.

52 Reg. UE 2022/2065. L'attuale approccio europeo è per lo più incentrato su interventi di *hard* e *soft moderation* preventivi e successivi sull' output algoritmico.

53 Il c.d. principio del *safe harbor*, prevede una sostanziale immunità determinata dal principio di esenzione della responsabilità per le conseguenze sociali e giuridiche delle pubblicazioni di terzi che avvengono per tramite di intermediari considerati neutrali (*providers exemption from liability*). Introdotto nella legislazione statunitense, con sezione 230(c)(I) del *Telecommunications Act* del 1996, ha trovato il suo *pendant* europeo nella *E-Commerce Directive* (dir. UE 2000/31) rimanendo sostanzialmente immutato fino all'entrata in vigore (*DSA* – Reg. 2022/2065). Concepito anni prima, dunque, dell'ascesa delle piattaforme digitali, perseguiva lo scopo di garantire un internet democratico e aperto, capace di autoregolamentarsi secondo il celebre principio del *free market of ideas* elaborato dal giudice O.W. Holmes nella *dissenting opinion* del caso *Abrams v. United States* del 1919. La sezione 230(c)(I) è stata da sempre interpretata, infatti, come uno dei «più importanti garanti della libertà di espressione su Internet»; cfr. J.M. Balkin, *Old School/New School Speech Regulation*, in *Harvard Law Review, Yale Law School, Public Law Research*, 491, 2014, 433.
Sulle origini della disciplina sulla responsabilità dei prestatori di servizi in Europa e negli Stati Uniti, si veda l'approfondita disamina di R. Petruso*, Le responsabilità degli intermediari della rete telematica. I modelli statunitense ed europeo a confronto,* Torino, XVIII, 2019.

54 Sulla distinzione nell'ambito della censura *de iure* tra «delega censoria funzionale» cioè imposta alle piattaforme a seguito di un provvedimento giudiziale/amministrativo, e «delega censoria sostanziale» che implica la

complessa operazione di bilanciamento dei diritti coinvolti nella «neo-intermediazione algoritmica»[55] del discorso pubblico su scala globale, ciò che non può sfuggire è come una regolamentazione orientata alla trasparenza procedurale, al *data due process*, come quella prevista nel *DSA*, per quanto cruciale, non sia, da sola, una sufficiente a risolvere gli squilibri informativi alla base del modello di business di piattaforma[56]. Affinché possa aversi una svolta nella costituzionalizzazione della rete che possa dirsi di natura «sostanziale» che non si attesti al solo livello «procedurale»[57], gli obblighi di trasparenza e *disclosure* devono essere affiancati e preceduti da una riflessione strutturale ed assiologica che permetta di definire il perimetro di liceità dell'estrazione dei dati alla base del funzionamento dei sistemi algoritmici di profilazione e quindi di moderazione dei contenuti operati dalle piattaforme.

Un' adeguata risposta alle sfide etiche e tecnologiche ai valori costituzionali sollevate dal funzionamento del *data mining* algoritmico tramite cui il *curatorial power*[58] delle piattaforme, tanto nelle sue forme esplicite *(hard moderation)* quanto nelle sue forme implicite o

valutazione sostanziale della liceità dei contenuti si veda M. Monti, *Privatizzazione della censura e Internet platforms: la libertà d'espressione e i nuovi censori dell'agorà digitale,* in *Rivista italiana di informatica e diritto*,1, 2019, 36 e ss.

[55] Per la definizione del concetto di «neo-intermediazione» si veda G. Giacomini, *Towards neo-intermediation. The power of large digital platforms and the public sphere*; 2018, in *Iride: Filosofia e discussione pubblica*, (3), 457-468, 2018. Sia consentito rimandare anche a I. de Vivo, *The "neo-intermediation" of large on-line platforms: Perspectives of analysis of the "state of health" of the digital information ecosystem.* in *Communications* 48, (3), 420-439, 2023 e in particolare, in merito alle accennate criticità relative alle possibili derive censorie di natura privata anche a seguito della disciplina introdotta dal *DSA*, Id. *Il potere d'opinione delle piattaforme-online: quale ruolo del "regulatory turn" europeo nell'oligopolio informativo digitale?*, in *Federalismi*, 2, 45-75, 2024.

[56] Per tali rilievi critici si veda A. J.R. Golia, *Beyond Oversight. Advancing Societal Constitutionalism in the Age of Surveillance Capitalism*, in *Int'l J. Const. L. Blog*, 2021; in particolare sugli aspetti lasciati in ombra dalla regolamentazione e cioè, la capacità dei dati di imporre ordini sociali attraverso la comunicazione e la narrazione relativa alle loro pratiche cfr. D. Nguyen, B. Beijnon, *The data subject and the myth of the 'black box' data communication and critical data literacy as a resistant practice to platform exploitation* 2023, *passim.*

[57] Il c.d. costituzionalismo procedurale, sarebbe la risposta necessaria e consequenziale alla natura globale di internet: non potendosi non prendere atto dell' asimmetria e della differenziazione dei modelli di protezione dei diritti fondamentali tra le due sponde dell'Atlantico, il linguaggio della tutela andrebbe cercato non nei valori costituzionali di natura sostanziale (che non possono non divergere), bensì nei meccanismi procedurali: «Sarebbe, dunque, la procedura, (gli obblighi di trasparenza algoritmica, il *data due process*) la parola chiave della nuova stagione del costituzionalismo digitale», così O. Pollicino il quale aggiunge che «se il costituzionalismo analogico è quello dei diritti sostanziali, quello digitale non può che fondarsi sulla dimensione meramente procedurale», cfr. O. Pollicino, *L'algoritmo e la nuova stagione del costituzionalismo digitale: quali le sfide per il giurista (teorico e pratico)?*, *in Giustiziainsieme.it,* 2021; Id. *La prospettiva costituzionale nell'era di internet*, in *Medialaws.eu*, 2019; id. *Judicial protection of fundamental rights on the internet: a road towards digital constitutionalism?,* Hart Publishing, 2021. Sempre sul «proceduralismo digitale» e sulla *global administrative law*, che vorrebbero trovare lo strumento utile a governare la globalizzazione nei meccanismi di review, negli obblighi di adeguata motivazione, nella trasparenza e nella responsabilità per le violazioni (cardini dell'impianto del DSA) si rinvia a M. Betzu, *I poteri privati nella società digitale*, *passim,* 180. A proposito di *procedural turn* si veda anche C. Bush, *The P2B Regulation (EU) 2019/1150: Towards a 'Procedural Turn' in EU Platform Regulation?*" in *Antitrust: Law & Policy eJournal,* 2020.
Cosi argomentando, l'unico argine, al momento ipotizzabile, alla sovranità funzionale esercitata dalle piattaforme infrastrutturali, farebbe perno su un controllo pubblico limitato alla correttezza e alla trasparenza del procedimento e quindi sul rafforzamento della responsabilizzazione dei big players digitali nel rispetto di tali obblighi.
Tuttavia, nonostante le inevitabili frizioni nello strumentario concettuale adottato dalle Corti tra le due sponde dell'Atlantico, riteniamo che la delega sostanziale alle piattaforme del bilanciamento dei diritti fondamentali e quindi della determinazione del loro contenuto concreto, a cui al momento si assiste, possa essere limitata, almeno nel contesto europeo, facendo appello all'efficacia orizzontale dei diritto fondamentali, che imporrebbe il loro rispetto anche da parte delle piattaforme nella loro autonomia contrattuale. In merito si veda almeno J. P. Quintais, N. Appelman, R. Fahy, *Using Terms and Conditions to Apply Fundamental Rights to Content Moderation*, in *German Law Journal,* 2022.

[58] R. Prey, *Locating Power in Platformization: Music Streaming Playlists and Curatorial Power*, in *Social Media + Society*, 6(2), 2020, 1.

«architetturali» (*soft moderation),* concretamente prende forma e si sviluppa[59], non può allora che passare dall' ampliamento del concetto di privacy fino a comprendere la tutela dell'identità personale *tout--court* contro indebite restrizioni ed interferenze epistemiche dovute alla governance algocratica delle esistenze. Se l'interferenza algoritmica si attesta al momento la determinazione dei «possibili epistemici», che della decisione costituiscono l'antecedente logico, la minaccia del trattamento automatizzato dei dati, personali e non, sulla libertà, o meglio, su quella che definiamo «identità epistemica individuale»[60] non è, allora, al momento facilmente identificabile come minaccia al diritto alla riservatezza come tradizionalmente concepito, né rientra nel concetto di profilazione vietata ai sensi del GDPR[61].

Partire da queste considerazioni significa, infatti, ripensare l'ontologia dei dati e la supposta distinzione tra ciò che è personale e ciò che non lo è -dicotomia questa- su cui si impernia l'attuale architettura del GDPR.

È necessaria, infatti, una nuova e diversa riflessione circa lo statuto da accordarsi non soltanto ai dati attualmente etichettati come personali, ma anche a tutti quei dati «esterni» ovvero metadati, dati di tracciamento, «scorie digitali» (ossia il sottoprodotto dell'interazione uomo-macchina)[62], la cui elaborazione, pur se priva, *prima facie*, di ricadute verificabili e immediate sulla sfera giuridica del singolo individuo (e per tanto esclusa dalla tutela apprestata dal GDPR) è destinata sul lungo termine a plasmare orizzonti decisionali, cognitivi e percettivi di individui e gruppi sociali, andando ad impattare a livello sistemico sul nucleo essenziale dei diritti a fondamento delle società democratiche.

Un tale mutamento di prospettiva nell'analisi, può orientare il legislatore e l' interprete ad individuare il trattamento giuridico da accordare ai dati, non più, o non soltanto, cercando di tracciare un pericolante confine tra ciò che è personale e ciò che non lo è, ma tentando di cogliere, in prospettiva dinamica, la «significatività» dell'impatto del loro trattamento algoritmico, sulla sfera dell'inviolabilità della persona: su quel nucleo duro di diritti che stando ai principi rinvenibili nelle tradizioni costituzionali europee, si ritiene vada a costituire la sfera intangibile dell'identità personale.

***3. il perimetro di tutela del «diritto all' identità personale» secondo il* GDPR.** Come visto, pur non confluendo in decisioni, i «suggerimenti algoritmici», ovvero, le decisioni di moderazione interne basate sul trattamento di dati personali e non personali, sono suscettibili di produrre effetti potenzialmente lesivi e discriminatori su interi gruppi sociali nel breve e nel lungo termine, incidendo in modi indiretti, ma non per questo meno significativi, sulla libertà di autodeterminazione. È il caso, ad esempio, dei citati fenomeni di *microtargeting,* ossia quella «somma di micro-violazioni individuali» che pur non confluendo in decisioni

[59] Sulla distinzione tra *hard moderation* o «moderazione in senso stretto» e *soft moderation,* si veda R. Gorwa, R. Binns, C. Katzenbach, *Algorithmic content moderation: Technical and political challenges in the automation of platform governance*, in *Big Data & Society,* 7, 2020, 3; sulla distinzione tra *content moderation* e *content curation,* cfr. P. Leerssen, *Seeing what others are seeing: Studies in the regulation of transparency for social media recommender systems,* Amsterdam, 2023, https://hdl.handle.net/11245.1/18c6e9a0-1530-4e70-b9a6-35fb37873d13.

[60] Per una più ampia riflessione in merito alle questioni sollevate dalla necessità di tutela della identità epistemica e dunque della libertà morale dell'individuo dalla sovradeterminazione algoritmica si rimanda ancora I. de Vivo, *Il sé allo specchio dell'algoritmo*, 2023, *passim.*

[61] Reg. UE 2016/67911

[62] È possibile, schematizzando, distinguere tre macro-categorie di dati: 1) *Volunteer data*: dati forniti volontariamente dagli utenti: 2) *Observed data*: dati acquisiti registrando le attività degli utenti; 3) *Inferred data*: dati dedotti dall'elaborazione delle precedenti categorie di dati (personali e non). si veda A. Pentland, D. L. Shrier, T. Hardjono, I. W.-Berger (a cura di*), Trusted Data: A New Framework for Identity and Data Sharing,* Cambridge, 2019. https://doi.org/10.7551/mitpress/12439.001.000.

suscettibili di incidere direttamente sulla sfera giuridica dell'interessato, sembrano, tuttavia, confliggere con quel «principio di non discriminazione per via algoritmica»[63] pur enunciato nel considerando 71 del GDPR[64].

Microtargeting, nudging algoritmico, così come le tecniche di profilazione psicografica citati, sono trattamenti automatizzati (di dati personali e non) che esulano dall'orizzonte applicativo della fattispecie di profilazione vietata dall'art 22 del GDPR per due ordini di motivi: la disposizione in parola, vieta il trattamento completamente automatizzato di dati esclusivamente nel caso in cui questo confluisca in una «decisione» produttiva di «effetti giuridici» sulla sfera giuridica singolo «interessato»; allo stesso tempo circoscrive ulteriormente la portata del divieto limitandone l'operatività al trattamento dei soli dati personali (come d'altronde la stessa disciplina dell'art. 15, che ne disciplina il diritto di accesso). Per questa via, va ad escludere dal suo raggio applicativo il trattamento di tutti i dati ricavati dalle operazioni di tracciamento e sorveglianza comportamentale[65]. In base a quanto finora argomentato, il nodo da sciogliere è il seguente: in che misura è ancora percorribile la strada della distinzione fra dati «interni» e «esterni», tra dati personali e meta-dati? Pur senza pretendere di elaborare uno statuto giuridico *ad hoc* per i dati c.d. esterni, non può prescindersi da un ripensamento della loro rilevanza giuridica oltre che economica, che non soltanto tenga conto del rischio sistemico legato al loro trattamento, ma che dall'altro lato, nel valutarne la rilevanza individuale, sia in grado di adottare come prospettiva controfattuale l'impatto su un emergente e più ampio concetto di «identità personale». In altre parole, è a partire dalla rilevanza e dalla significatività del loro impatto sull'integrità dell'identità individuale, compresa in tutte le sue dimensioni (dimensione epistemica, socio-relazionale, morale) che è possibile disegnare il perimetro di tollerabilità e quindi di liceità della loro raccolta e sfruttamento, tanto da parte di attori privati, quanto da parte di attori pubblici. Peraltro, in virtù dell'efficacia orizzontale riconosciuta ai principi fondamentali della Carta europea, tanto dalla giurisprudenza della CGUE, quanto dalla corposa giurisprudenza della Corte EDU in materia[66], l'autonomia privata delle piattaforme nel definire il proprio «statuto ordinamentale

---

[63] Per l'elaborazione del principio si veda S. Simoncini, A. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale,* 2019, *passim,* 102.

[64] Sulla strutturale debolezza del GDPR, nel garantire la tutela sia a livello micro che a livello macro, si veda S. Scagliarini, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in: *Consulta Online* 2, 335-371, 2021.

[65] Sulle varie tipologie di dati da cui è tratto il *surplus* e la sorveglianza comportamentale si veda *supra,* nota 62.

[66] La Convenzione Europea e la giurisprudenza della Corte EDU fa sistema con l'interpretazione della CDFUE che ad essa espressamente si collega per via dell'art 52 ph. (3) secondo cui: Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell'Unione conceda una protezione più estesa. Per approfondimenti in merito, si veda A. Ruggeri, *La Carta di Nizza-Strasburgo nel sistema costituzionale europeo*, in *Rivista AIC*,3/2020. La giurisprudenza di entrambe le Corti, nel confermare la possibilità di esercitare orizzontalmente, nei confronti dei poteri digitali privati, i diritti protetti Carta dei diritti fondamentali dell'Unione europea si è concentrata in particolare sull'estensione del diritto alla libertà di espressione nella moderazione dei contenuti online e il relativo bilanciamento dei diritti potenzialmente confliggenti delle altre «parti coinvolte» diverse dall'utente, che trovano tutela nella Carta (quali la tutela della vita privata ex art.7, il diritto alla protezione dei dati personali ex art.8, il diritto alla non discriminazione ex art.21): *ex multis*, si veda: *Bédat c. Svizzera*, App. No. 56925/08, para. 52 (29 marzo 2016), https://hudoc.echr.coe.int/eng?i=001-161898; in relazione al *revenge porn: Volodina v. Russia* (n.2), App. No. 40419/19, par. 50-68 (14 settembre 2021), https://hudoc.echr.coe.int/eng?i=001- 211794; sentt. C-345/17, *Sergejs Buivids c. Datu valsts inspekcija*, -ECLI-:-EU-:C:2019:122, para. 65 (14 febbraio 2019). Per quanto riguarda l'applicabilità della giurisprudenza della Corte europea dei diritti dell'uomo sulla libertà di espressione, *ex multis* causa C-401/19, *Polonia/Parlamento e Consiglio* (15 luglio 2021) e, in particolare, le Conclusioni dell'Avvocato generale Øe, causa C-401/19, *Polonia/Parlamento e Consiglio* (15 luglio 2021); *Palomo Sánchez et al. c. Spagna*, App. No. 28955/06, para. 59 (12 settembre 2011),

interno» - può - e deve essere legittimamente considerata suscettibile di limitazione da parte del potere pubblico, laddove vada ad comprimere la tutela del nucleo essenziale dei diritti inviolabili, andando a toccare, come può accadere, il meta-principio della dignità che permea l'intero assetto costituzionale europeo.

Parallelamente a ciò, rendere consapevoli gli utenti, attraverso interventi volti alla costruzione di un'alfabetizzazione mediatica critica (*critical data literacy*)[67], del rapporto originario e costitutivo tra dati (generati consapevolmente o meno) e identità – e quindi tra tutela della *privacy* intesa in senso ampio quale «libertà intellettuale»[68] e diritto al pieno sviluppo della propria personalità, è precondizione di efficacia di qualsiasi tattica di governance che si prefigga di scongiurare il rischio che l'egemonia culturale veicolata dall'IA sconfini in un vero e proprio «colonialismo cognitivo». Si tratta del primo passo per pensare ad una ri-politicizzazione del modello aziendale di «capitalismo della sorveglianza»[69] o meglio di quel «realismo della sorveglianza»[70]che legittima, normalizzandoli, i presupposti epistemologici che rendono possibile la manipolazione sistemica degli individui e le relative conseguenze sulla tenuta delle istituzioni democratiche.

A ben vedere la depoliticizzazione di problemi strutturali è in generale insito alle forme della c.d. *Limited government regulation* (*LGR*[71]) a cui è ascrivibile il nuovo quadro regolatorio europeo.

Rimedi strutturali, richiederebbero di sondare, altresì, le soluzioni percorribili a livello transnazionale per ripensare le politiche alla base dell'estrazione massiva di dati che fino ad oggi, nel contesto anomico della rete, non ha trovato limitazioni di sorta. I dati, come detto, per lungo tempo sono stai concepiti come *res nullius* liberamente disponibili all'appropriazione tanto da parte delle piattaforme, quanto, per loro tramite – come le dichiarazioni Snowden[72] hanno drammaticamente rivelato- da parte dei governi per ragioni

---

https://hudoc.echr.coe.int/eng?i=001- 106178. Recentemente C-140/20, G.D. v. *Commissioner of An Garda Síochána et al.*, ECLI:EU:C:2022:258, para. 49 (5 aprile 2022), https://curia.europa.eu/juris/liste.jsf?num=C-140/20; *Remuszko v. Poland,* App. No. 1562/10 (16 luglio 2013), https://hudoc.echr.coe.int/eng?i=001-122373.

[67] T.P. Nichols, A. Smith, S. Bulfin, A. Stornaiuolo, *Critical literacy, digital platforms, and datafication,* in J.Z. Pandya, R.A. Mora, J. Alford, J., N.A. Golden, R.S. de Roock, (Eds.), *The Handbook of Critical Literacies. Routledge,* 2021.

[68] Cfr. S. Eskens, *The personal information sphere: An integral approach to privacy and related information and communication rights,* in *Assoc Inf Sci Technol.* 71, 1116-1128, 2020. Sulla teorizzazione della *privacy intellettuale* si veda N.M. Richards*, Intellectual privacy: Rethinking civil liberties in the digital age*, Oxford, 2015.

[69] Su cui S. Zuboff, *The age of surveillance capitalism:* 2019, *passim.*

[70] Si veda L. Dencik, *Surveillance realism and the politics of imagination: Is there no alternative?,* in *Krisis.* 1-3, 2018.

[71] Con l'espressione menzionata si fa riferimento all'applicazione di standard legalmente definiti per la condotta del settore da parte delle autorità pubbliche sotto forma di: (a) responsabilità concordata *(co-regulation*); (b) responsabilità stabilita per legge *(regulation set by law*), cfr, M.E. Kraft, S.R. Furlong*, Public policy: Politics, analysis and alternatives,* 2013. Esempi di questo modello sono: (a) la *Loi Avia* francese (n. 2020-766); (b) il *NetzDG* tedesco (*Network Enforcement Act*, 2017) precedenti all'entrata in vigore del reg. UE 2022/2065 (*DSA*).

Per un'analisi diacronico-comparativa dei modelli europei di *platform governance* si veda: E. De Blasio, D. Selva *Who is responsible for disinformation? European approaches to social platforms' accountability in the post-truth era,* in *American Behavioral Scientist*, 65(6), 825-846, 2021. Si veda anche A. Rochefort, *Regulating social media platforms: A comparative policy analysis, i*n *Communication Law and Policy*, 25(2), 225-260, 2020. K.S. Rahman*, Regulating informational infrastructure: Internet platforms as the new public utilities*, in *Georgetown Law and Technology Review,* 2(2), 234-248, 2018. Per un'analisi comparativa basata sul criterio di espansività delle politiche si rimanda anche a I. de Vivo*, The "neo-intermediation" of large on-line platforms*, 2023, *passim,* 8.

[72] Nel 2013, Edward Snowden, ex collaboratore della National Security Agency (NSA) degli Stati Uniti, con la divulgazione di una vasta quantità di documenti riservati, ha reso globalmente nota l'esistenza di programmi di sorveglianza di massa che consentivano alla NSA di raccogliere dati su comunicazioni telefoniche e attività su internet di milioni di persone, cittadini e leader politici, statunitensi e non, innescando il primo dibattito di risonanza globale su trasparenza dei poteri governativi nel digitale e sicurezza nazionale. Non può che rimandarsi all'autobiografia di Snowden: *E. Snowden, Permanent record,* 2019, nonchè S. Landau, *Making Sense from*

di sicurezza nazionale. La seconda parte del lavoro, analizzerà dunque come le varie declinazioni di sicurezza nazionale, attualmente, possano frapporsi alla realizzazione di una *data governance* globale costituzionalmente orientata, mettendo in luce la natura «strategicamente duale» dei big-data.

4. La valenza duale dei dati: i dati come asset strategico e il «capitalismo politico» statunitense. Se la raccolta e l'uso dei dati, rappresentano una minaccia al nucleo essenziale dei diritti individuali, mettendo a rischio direttamente e indirettamente la resilienza e il corretto funzionamento degli istituti democratici, al tempo stesso sono da considerarsi a tutti gli effetti come un *asset* decisivo per la sicurezza nazionale: i dati infatti sono il motore dell'innovazione tecnologica nella sua duplice valenza civile e militare, costituendo condicio sine qua non dell'implementazione dell' IA anche in campo bellico.

In ragione, allora, dell'equivalenza progressiva tra controllo e gestione dei dati e autonomia geostrategica, nel quadro geopolitico internazionale si assiste ad un movimento centripeto e, per certi versi opposto alla globalizzazione, che vede forme di rivendicazione della sovranità territoriale esprimersi attraverso il tentativo di nazionalizzazione dei dati e questo tanto in regimi autoritari, quanto in Stati democratici[73].

Citando ancora la raccomandazione di Schmidt:

«Saranno i dati ad alimentare i prossimi conflitti globali. L'accuratezza, la letalità e la velocità, dipende da immense serie di dati carburante che alimenta il motore del Machine Learning (ML) […] Chi accumula e organizza per primo il maggior numero di dati avrà la superiorità tecnologica, quindi spetta al Dipartimento raccogliere, archiviare, condividere, analizzare e proteggere i propri dati più velocemente e meglio dei suoi concorrenti. I dati devono essere considerati come una delle risorse più potenti nell'arsenale del Dipartimento»[74].

Una visione questa, che spiega bene come i dati estratti sul territorio di uno Stato (o meglio dalle popolazioni che lo abitano) generino non soltanto remunerazione del capitale, ma anche plusvalore di potere statale in termini di autonomia geostrategica e sicurezza[75] .

Come detto, si tratta di un aspetto fondamentale da tenere in considerazione, per vagliare l'efficacia e l'applicabilità a livello regionale e globale del nuovo quadro regolamentare dell'UE in materia di data governance: la stretta relazione tra raccolta dati e sicurezza nazionale, mette infatti in evidenza gli ostacoli, che in ossequio al principio di sovranità territoriale, si frappongono alla realizzazione di una data governance di «marca europea».

Attraverso una tattica di governance che fa perno sulla «categoria del rischio»[76] quale

---

Snowden: what's significant in the NSA surveillance revelations, in *IEEE Security & Privacy,* 11(4), 54-63, 2013; A. Wiener, *Uncanny Valley: Seduction and Disillusion in San Francisco' Startup Scene*, London, 127, 2020.

[73] Sul tema F. Balestrieri, L. Balestrieri, *Guerra digitale: il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico,* Roma, 2019; N. Möllers, *Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State,* in *Science, Technology, & Human Values*, 46(1), 112-138, 2021.

[74] E. Schmidt, *Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis passim,* 1.

[75] F. Balestrieri, L. Balestrieri, *Guerra digitale: il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico,* 2019 *passim.*

[76] Tecnicamente il rischio è una combinazione tra la probabilità che si verifichi un determinato pericolo e l'entità delle conseguenze che tale pericolo può comportare cfr. R. Gellert, *The Risk-Based Approach to Data Protection,* Oxford, 2020. Per l'analisi della differenza t*ra risk approach e risk based approach* di vedano: G. De Gregorio, P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age* (59(2), in *Common Market Law Review*, 473-500*,* 2022: mentre la regolamentazione del rischio *strictu sensu* è identificabile come una «interferenza governativa con i processi di mercato o sociali per controllare le potenziali conseguenze negative», la «regolamentazione basata sul rischio» utilizza il *frame* come strumento per dare priorità e indirizzare l'azione di contrasto in modo proporzionato al pericolo effettivo: in altre parole, tenderebbe a «calibrare» l'applicazione della legge sulla base di punteggi di rischio concreti.

principale *proxy* trasduttiva[77] tra «costituzionalismo sociale»[78] e «costituzionalismo politico»[79]il GDPR, pur con le sue rilevate limitazioni tanto a livello micro, quanto a livello macro (nella gestione dei big data), si è rivelato strategicamente efficace imponendosi come *benchmark* a livello mondiale nella tutela dei diritti. Nonostante ciò, il GDPR sembra scontare l'assenza di una politica euro-unitaria in materia di trasferimento e monetizzazione dei dati[80]. La mancata elaborazione di una prospettiva strategica comune, rischia, infatti, di comprometterne l'effettivo perimetro di efficacia nella misura in cui rende di difficile interpretazione concetti quali «sicurezza nazionale» e «interesse geopolitico» che, come espressamente previsto dal considerando 16 dello stesso regolamento, definiscono i limiti di applicazione della normativa[81].

Dato lo stretto legame-che intercorre tra raccolta dati e sicurezza e in ossequio al principio di sovranità territoriale, la concreta applicabilità della normativa europea non può che dipendere dai modi in cui il diritto positivo e la giurisprudenza definiscono la regolazione della sicurezza in ambito nazionale, trovando geometria ed estensione variabile a seconda dell'effettivo bilanciamento tra questa e la tutela dei diritti individuali fondamentali nei rispettivi ordinamenti.

Il citato considerando 16, permettendo infatti ai singoli Stati Membri di non attuare la normativa quando ad essere in ballo sono la sicurezza nazionale e /o l'interesse geopolitico, ben può legittimare l'eventuale condivisione di dati con Paesi terzi tramite accordi bilaterali (c.d. *free riding),* anche quando, come nel caso statunitense, obiettivi e standard in materia di *data-protection* appaiono incompatibili con l'approccio europeo[82].

Ciò significa che gli standard di tutela così come pensati dalla UE nel *framework* del costituzionalismo digitale, anche in ambito regionale, dovranno confrontarsi con differenti impianti costituzionali e obiettivi strategici delle democrazie d'oltreoceano, che vedono il rapporto tra sicurezza nazionale - in particolare le esigenze governative di accesso e raccolta dati e tutela dei diritti individuali - una partita a somma zero.

Sfruttando quanto richiamato dal considerando 16 del Regolamento e in ragione della crescente tensione sino-americana nella sfida per la sovranità tecnologica, gli Stati Uniti

---

[77] La categoria del rischio è utilizzata a partire dal GDPR e con declinazioni parzialmente diverse con il DSA l'AI-Act, come principale tecnica di governance adottata dalla l'UE per promuovere i diritti fondamentali e i valori democratici come contro-limiti al predominio delle pure logiche di mercato nella società algoritmica. In quanto tattica caratterizzata dall'obiettivo di bilanciare adeguatamente la necessità di tutelare i diritti e le libertà fondamentali nell'ambiente digitale, proteggendo al contempo le libertà economiche, quali motori di innovazione e fondamentali per il Mercato Unico Digitale l'obiettivo non sarebbe quello di minimizzare i rischi in tutti i costi imponendo precauzioni massime (c.d. costituzionalismo precauzionale), ma raggiungere quella che è definibile come un' ottimizzazione del rischio (*consitutional optimization)* cfr. A. Vermeule, *The Constitution of Risk*, Cambridge, 2014. Sul tema, si rimanda ancora a G. De Gregorio, P. Dunn, *The European Risk-Based Approaches, Connecting Constitutional Dots in the Digital Age*, 2022, *passim,* 21.

Parallelamente, attraverso la definizione normativa dei livelli di rischio accettabile, il tentativo è quello di dotare di efficacia i principi elaborati nel *framework* di un costituzionalismo «spontaneo», come appunto il costituzionalismo digitale, tramite il recupero dalla centralità del momento politico (*Political costitutionalism*) e, segnatamente, della deliberazione democratica nell'amministrazione dei diritti fondamentali, riaffermando un modello basato sul ruolo delle istituzioni democratiche.

[78] Sulle caratteristiche del «costituzionalismo digitale» si veda *supra,* nota 12.

[79] Sul concetto di «costituzionalismo politico» si veda *supra* nota 10.

[80] A dettare le prime regole in materia di *data monetization* il *Data Act*, reg. UE 2023/2854 e il *Data Governance Act* (DGA) reg. UE 2022/868.

[81] In merito si veda G. De Ruvo*, Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma,* 2022*, passim.*

[82] Sulle ragioni che giustificano la necessità di rafforzare la sovranità tecnologica europea a scapito di quella degli Stati membri si veda M.E. Bartoloni, *La politica di sicurezza e di difesa comune dell'UE: verso un'"autonomia strategica" o "strategie in autonomia"*?, in *Le Istituzioni del federalismo*, 1-2, 2022, *passim*.

tendono, infatti, a non considerare l'UE come un'unica entità, ma a cercare di attrarre nella propria orbita i singoli Paesi membri: è sempre Schmidt a proporre – in funzione anticinese – un'alleanza delle «tecno-democrazie» composta da singoli Stati europei che – riconoscendo la minaccia alla sicurezza nazionale dovuta allo sviluppo cinese – decidano di integrare i dati che vengono raccolti nel loro territorio con l'amministrazione americana, sostanzialmente bypassando la normativa GDPR[83].

Del resto, dal canto loro, se gli Stati Uniti procedessero a regolamentare il flusso di dati che le grandi aziende del digitale raccolgono, limitandone l'accesso alle big tech o introducendo dei paletti simili a quelli del GDPR, l'innovazione tecnologica americana subirebbe un clamoroso rallentamento lasciando il primato indiscusso alla Cina[84]. Emblematica rappresentazione della divergenza di obiettivi tra «capitalismo politico» americano[85] nel mercato dei dati e approccio europeo è il rapporto finale della Commissione Nazionale di Sicurezza (NSA) sull'IA:

«il governo federale deve lavorare insieme alle aziende americane per mantenere la leadership americana e per supportare lo sviluppo di diverse applicazioni dell'intelligenza artificiale che possano portare avanti l'interesse nazionale nel senso più ampio possibile […] aggregando – sia da un punto di vista quantitativo, sia da un punto di vista infrastrutturale – i dati raccolti dalle big tech con quelli raccolti da agenzie federali come la National Security Agency» [86].

La differenza con il GDPR è evidente: obiettivo principale del governo statunitense non è quello di garantire la protezione dei dati dell'individuo, ma primariamente quello di collaborare e sfruttare il potenziale tecnologico delle *big-tech* in prospettiva di supremazia strategico-militare attraverso il progressivo rafforzamento del «patto tecnocratico» tra Silicon Valley e gli apparati governativi.

In ragione dunque del progressivo processo di fusione tra la sfera militare e la sfera civile nell'ambito del *data mining*, poco spazio sembra rimanere a disposizione per istanze quali *accountability,* trasparenza e protezione dei diritti individuali.

Anche gli strumenti giuridici a disposizione nell'ordinamento statunitense, (quali *Committee on Foreign Investments in the US* (CFIUS) e l'*International Emergency Economic Powers Act* (*IEEPA*) vengono, infatti, utilizzati in prospettiva strategica e giustificati dalla retorica securitaria. Se i dati sono da considerarsi a tutti gli effetti come un asset decisivo per la sicurezza nazionale in ragione della loro rilevanza in campo bellico, le aziende straniere che li raccolgono a priori verranno considerate «infrastrutture critiche»[87]. Ciò significa che per operare negli USA –

[83] Cfr. E. Schmidt, *China Strategy Group Asymmetric Competition: A Strategy for China & Technology*, *Internet archive,* 25-27, 2020;

[84] Su questo rischio si veda ancora E. Schmidt, *China Strategy Group,* 2020, *passim.* Sul tema si veda G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma,* 2022, *passim.*

[85] Il concetto di «capitalismo politico» coniata da A. Aresu pone l'accento sulla compenetrazione di economia e politica in un «tutto organico» che si verifica a più livelli e secondo diverse modalità nelle economie più avanzate: come simbiosi di Stato e partito comunista in Cina; come presenza di numerosi apparati burocratici deputati alla sicurezza nazionale negli Stati Uniti, con la loro panoplia di poteri di emergenza; come utilizzo a scopi politici della tecnologia e delle grandi imprese tecnologiche nella competizione internazionale; come capacità di definire industrie e settori strategici da sostenere e di aziende 'nemiche' da avversare per la loro collocazione geopolitica; come capacità delle grandi potenze di guardare alle proprie economie secondo l'ottica della sicurezza nazionale; cfr. A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, Milano, 2020. Su obiettivi e sfide del nuovo capitalismo politico americano e sulla crescente similitudine di strategie tra Stati Uniti e Cina si veda; A. Dworkin, M. Leonard, *Can Europe save the world order?,* in *ecfr.eu*, 2018.

[86] *National Security Commission On Artificial Intelligence, Final Report,* 2021, 263.

[87] I concetti di infrastruttura critica e di sicurezza nazionale su cui si basa il blocco degli investimenti, evolvono ridefinendosi continuamente, sulla base delle nuove tecnologie e dei nuovi obiettivi geostrategici che le potenze cercano di perseguire, e pertanto sono impossibili da definire a priori*:* «la sicurezza nazionale, per un impero, è

dovranno passare necessariamente per un'istruttoria del CFIUS che può concludersi con *executive order* del presidente (non sindacabile a livello giurisdizionale) o che comunque saranno soggette al perimetro di applicazione dallo IEEPA utilizzabile appunto «per affrontare una particolare e straordinaria minaccia [...] alla sicurezza nazionale, alla politica estera, o all'economia degli Stati Uniti»[88].

Paradigmatica, al riguardo, è la vicenda che ha coinvolto *TikTok*[89] in cui gli USA hanno consapevolmente deciso di utilizzare lo IEEPA in funzione anti-cinese, con la decisione di *bannare* la piattaforma. A ben vedere, infatti, il c.d. *ban* non è che l'*extrema ratio* messa a disposizione dallo IEEPA, che dal punto di vista normativo, prevede anche soluzioni intermedie, quali ad esempio, la possibilità di congelare un asset fino a quando esso non rispetti le condizioni dettate dagli USA. Come giustamente rilevato, lo strumento poteva quindi essere utilizzato come deterrente, per imporre, ad esempio, alla Cina l'obbligo di rendere i server open access- aprendo la strada ad un effettivo processo di regolazione e trasparenza del flusso di dati. Soluzione tuttavia, che sembra esser stata scartata *ab origine*, presumibilmente per l'effetto domino che un tale precedente avrebbe potuto innescare, nella misura in cui avrebbe esposto la raccolta dati americana ad istanze identiche da parte di altri Paesi, compromettendone la raccolta dati[90]. Lo IEEPA è stato al contrario utilizzato come arma geo-economica nel tentativo di forzare la vendita di *TikTok* ad un'azienda statunitense con l'obiettivo di continuare ad estrarre dati, tramite il più avanzato l'algoritmo della piattaforma cinese, ma assicurandone la proprietà americana[91] . La tutela dei diritti individuali non è un problema che sembra sia entrato a far parte del ragionamento.

5. Riflessioni conclusive. L'uso politico di strumenti giuridici come il CFIUS e lo IEEPA si basa sulla dicotomia oppositiva tra tutela dei diritti individuali e sicurezza, quale presupposto ideologico della normalizzazione della sorveglianza pubblica e privata.

Negli USA la prevalenza delle esigenze governative di raccolta dati per lo sviluppo dell'IA sui diritti individuali è legittimata da una narrazione che – coadiuvata da una atmosfera di normalizzazione efficacemente descritta in letteratura come realismo di sorveglianza[92] – vede la sicurezza nazionale quale *knock-out* prevalente sulla tutela dei diritti individuali. Una visione aprioristica che snaturando l'idea stessa di bilanciamento quale *processo* attuale e dinamico che attende e pretende attualizzazione secondo i criteri di proporzionalità, si presta a strumentalizzazioni a livello politico volte a giustificare limitazioni anche estreme della libertà personale.

---

ciò che esso vuole che sia per mantenersi», cfr. A. Aresu, *Le potenze del capitalismo politico. Stati Uniti e Cina*, 2020, *passim,* 116. In ambito europeo si veda il reg. UE 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione, in settori strategici che possono incidere sulla sicurezza o sull'ordine pubblico, in GUUE L 79I del 21 marzo 2019, 1.

[88] *US Code, Unusual and extraordinary threat; declaration of national emergency; exercise of Presidential authorities, title 50, chapter 35, section 1701.* È chiaro che il punto problematico, evidentemente, è la nozione di sicurezza nazionale: è possibile inquadrarla normativamente? Come si fa a definire «critica» un'infrastruttura?

[89] La piattaforma nasce dall'acquisizione da parte di Bytedance dell'azienda MUSICalLY, anch'essa cinese, ma con sede a S. Francisco circostanza questa che ha reso utilizzabile lo IEEPA potendo considerare l'operazione un investimento straniero in territorio americano. Per un'approfondita analisi del caso, si rimanda ancora a G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma,* 2022, *passim.*

[90] Così G. De Ruvo, *Raccolta dati, intelligenza artificiale e sicurezza nazionale: l'uso geopolitico degli strumenti giuridici americani come freno alla data governance globale. Il caso TikTok come paradigma,* 2022, *passim*, 7, secondo cui lo scopo primario sarebbe stato esattamente quello di garantire che i dati vadano ad implementare «l'IA a stelle strisce» e non quella cinese.

[91] Si veda H, Kissinger E. Schmidt, D. Huttenlocher, *The Age of AI and Our Human Future,* London, 2021.

[92] L. Dencik, *Surveillance realism and the politics of imagination: Is there no alternative?*, 2018, *passim.*

Il caso americano è allora paradigmatico e può e deve fungere da monito per ampliare la riflessione sul concetto in perenne metamorfosi di sicurezza così come inteso tanto in ambito nazionale, quanto in ambito europeo e sui criteri che ne informano il processo di attualizzazione.

Se è vero, stando ai principi informatori della *data strategy* promossa dalla UE, che qualsiasi compressione della sfera della privacy , da intendersi come detto, in senso ampio ossia quale diritto all'identità individuale, deve fondarsi su una base giuridica adeguatamente accessibile (trasparente) prevedibile e formulata in modo sufficientemente chiaro da poter essere compresa, e dati gli attuali limiti posti dalla sovranità statale, il modo in cui il diritto positivo e la giurisprudenza vi accorderanno tutela nel bilanciamento con le ragioni dei sicurezza, non solo incide sulla complessiva struttura del sistema politico e giuridico del Paese, ma può determinare in concreto anche la compatibilità dei sistemi in questione con il fulcro dell' identità internazionale europea.

Il framework del «costituzionalismo digitale sostanziale» che di tale identità è espressione, è infatti non solo fattore di legittimazione della sovranità digitale europea che in esso trova fondamento, ma è prisma ermeneutico essenziale per valutare, anche tra le attività di *free riding* degli Stati membri, cosa possa considerarsi legittimo e cosa invece, sfidando il fulcro dell'identità internazionale europea, sia inquadrabile nella cornice della de-europeizzazione.

Per rispondere alla domanda circa la configurabilità di una sorveglianza o meglio di una data-veglianza pubblica e privata che, sebbene operativa nell'interesse della comunità, non sia lesiva dei diritti fondamentali del singolo, sono due, infatti, gli aspetti che si è cercato di mettere in rilievo nel corso della trattazione. La necessità da un lato, di pensare ad una ri-politicizzazione del modello aziendale che informa il *big data capitalism,* e che legittima, normalizzandoli, i presupposti epistemologici della datificazione. Affinchè ciò sia possibile si ritiene necessario *in primis* delegittimare l'ontologia ivi sottesa, ossia la visione dei dati come «risorsa naturale» liberamente disponibile all'appropriazione. Si tratta, infatti, del primo passo per ripensare alla rilevanza etico-giuridica, oltre che economica, di metadati e «*surplus* comportamentale», superando l'ormai fumosa distinzione nell'universo digitale di ciò che è personale e ciò che non lo è. A tale cambio di prospettiva non può non accompagnarsi un ripensamento in senso evolutivo del concetto di *privacy*, atto a comprendere una più ampia riflessione sul concetto di identità personale, presupposto indefettibile del libero agire, quale «sfera di propagazione» in cui tutti i diritti e i principi che informano la Carta europea e la Convenzione EDU si connettono tra loro, rinforzandosi reciprocamente. Diritti quali il rispetto della privacy e della riservatezza delle comunicazioni (artt. 8 CEDU e 7 CDFUE), la libertà di pensiero (artt. 9 CEDU e 10 CDFUE), la libertà di espressione, nella sua dimensione attiva e passiva, (artt. 10 CEDU e 11 CDFUE), così come interpretati e applicati dalle le ricostruzioni giurisprudenziali delle rispettive Corti, sembrano, infatti, interagire nella più ampia dimensione di quella che definiamo «la sfera dell'identità personale». Detto con le parole di Janneke Gerard, il carattere speciale dei diritti fondamentali può essere paragonato a quello di un prisma: «un diritto fondamentale è trasparente e sembra un oggetto chiaramente definito, ma non appena la luce lo colpisce e lo attraversa, diventa visibile un ampio spettro di colori»[93]. Nel tempo i lati del prisma di un diritto fondamentale, rifletteranno aspetti precedentemente nascosti alla percezione: nuovi interessi, valori e diritti che seppur

[93] «Il diritto quindi si disperde in uno spettro di colori, di interessi, di valori e anche di più diritti. Tutti questi [colori] possono essere visti e nominati individualmente, ma non possono non mescolarsi tra loro. Ai due lati dello spettro, inoltre, ci sono colori che non sono visibili a occhio nudo, ma che sono chiaramente presenti». cfr. J. Gerard, *The prism of fundamental rights*, in *European Constitutional Law Review,* 8:2, 173-202, 2012, 178, tr. Nostra.

diversi e nominabili individualmente, sono difficilmente separabili e di cui non può non tenersi conto nella svolta verso la regolazione «umano-centrica» su cui l'Europa è intenzionata a definire la propria «identità nel digitale».
Il secondo aspetto messo in evidenza, di rilievo strutturale, spinge a interrogarsi sulle possibilità effettivamente offerte dall'attuale architettura costituzionale dell'Unione all'acquisizione e alla costruzione di quell' autonomia strategica presupposta alla sovranità digitale, e necessaria a dotare di effettività una data governance costituzionalmente orientata. Il c.d. approccio integrato[94] delle competenze in materia di sicurezza promosso dalla UE, sarebbe, infatti, praticabile nella misura in cui l'UE potesse utilizzare il complesso di poteri d'azione nell'ambito di un sistema di obiettivi complessivamente considerato, secondo una visione olistica e comune. Tuttavia, in un ordinamento come quello dell'Unione, fondato su una rigida ripartizione di competenze[95], una visione integrata delle varie politiche si porrebbe inevitabilmente in contrasto con il principio d'attribuzione[96] su cui l'assetto impresso dai Trattati all'architettura costituzionale dell'UE continua a fondarsi. In questa prospettiva, il processo di acquisizione di autonomia strategica nel settore della sicurezza appare, dunque, ostacolato dallo stesso assetto costituzionale, che impedisce di concepire l'ordinamento dell'Unione come entità unitaria[97]. Come si è cercato di porre in evidenza nel corso dell'analisi, riconoscere all'UE le prerogative necessarie perché si possa parlare di sovranità digitale europea, è allora precondizione alla realizzazione di un costituzionalismo digitale non soltanto procedurale, ma anche sostanziale.

[94] Secondo il Consiglio europeo l'autonomia strategica è concepita come capacità dell'Unione di consolidare la propria dimensione di sicurezza e difesa attraverso il ricorso al complessivo ventaglio di meccanismi e strumenti messi a disposizione dall'ordinamento UE, quindi attraverso un approccio c.d. integrato*:* «Per attuare efficacemente l'approccio integrato dell'UE utilizzeremo appieno e coerentemente tutte le politiche e tutti gli strumenti dell'UE disponibili, oltre a ottimizzare le sinergie e la complementarità tra sicurezza interna ed esterna, sicurezza e sviluppo nonché le dimensioni civile e militare della nostra politica di sicurezza e di difesa comune (PSDC)», cfr. CE*, Una bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali*, Bruxelles, 21 marzo 2022, 13. https://data.consilium.europa. eu/doc/document/ST-7371-2022-INIT/it/pdf

[95] Sulla natura «perdente» della logica della separazione delle competenze in ragione degli ambiti materiali oggetto di regolazione, si veda Ruggeri, che sottolinea necessità loro integrazione ispirata al modello costituzionale connotato da discipline positive per gradi decrescenti di generalità; cfr. A. Ruggeri, *Sovranità e autonomia regionale, dal modello costituzionale al tempo dell'emergenza (prime notazioni)*, 2021, *passim,* 130.

[96] La possibilità di temperare la logica del riparto delle competenze con il principio di sussidiarietà sullo sfondo di una legittimazione della sovranità «orientata ai valori» costituirebbe, ad oggi, la condizione di possibilità di quell'eterogenesi dei fini che se da un lato estende la capacità di penetrazione della fonte europea nel diritto interno, dall'altro legittima quel cambio di prospettiva strategica, dichiarato a chiare lettere nel 2020 dalla Presidente della Commissione Von der Leyen, che vede la UE trascendere l'idea di mercato unico come fine in sé, puntando, piuttosto, alla creazione di standard europei con un impatto globale. Tra i principali obiettivi come detto, vi è quello di creare un modello alternativo di trasformazione digitale, come terza opzione nelle attuali battaglie geopolitiche e geoeconomiche tra Stati Uniti e Cina; cfr. Commissione europea, *Dare forma al futuro digitale dell'Europa.* COM (2020) 67; Commissione europea, *2030 Bussola digitale: La via europea per il decennio digitale,* COM (2021) 118; in merito si veda G. Glasze, F.Dammann, M. Münßinger, D. Danet, C. Bômont, A. Desforges, *Reception and Elaboration of "Digital Sovereignty" in Three European Discourse Arenas: France, Germany, and the EU,* in G. Glasze, et al. *passim,* 2023; C. Hobbs, Europe's *digital sovereignty: From rulemaker to superpower in the age of US- China rivalry* in *London: European Council on Foreign Relations*, 2020. T. Christakis, *European digital sovereignty': Successfully navigating between the 'Brussels effect' and Europe's quest for strategic autonomy*, in *SSRN Journal 7,* 2020.

[97] Sul tema si veda ampiamente M.E. Bartoloni*, La politica di sicurezza e di difesa comune dell'UE: verso un'"autonomia strategica" o "strategie in autonomia"?,* 2022, *passim*, il quale osserva come l'attuale pilastro PSDC, anche nella prospettiva di un suo ulteriore potenziamento, non potrà prescindere dalle politiche materiali (ex politiche comunitarie) e dalle dinamiche del mercato interno, che la Commissione, qualifica come «mercato europeo della difesa»; Cfr. Comunicazione della Commissione COM (2022) 60 *final*, *passim.*

Abstract. La capacità di ogni Stato di definire autonomamente il proprio quadro regolamentare concernente l'economia digitale, il potere di controllo sulle infrastrutture strategiche, sicurezza informatica e disinformazione costituiscono l'attuale sfida «esistenziale» che gli ordinamenti democratici si trovano ad affrontare.
In questo scenario, la strategia dell'Unione per costruire la c.d. «sovranità digitale europea» rappresenta il tentativo dell'Europa di riaffermare la propria identità normativa-valoriale a livello geopolitico in linea con le sue radici etiche e costituzionali. A seguito di un breve inquadramento delle caratteristiche salienti del c.d. costituzionalismo digitale, nel cui frame teorico si inserisce e va letta l'attuale svolta normativa europea per la «sovranità digitale», un focus specifico sarà dedicato all'analisi della questione trasversale e preordinata a qualsiasi tentativo di regolazione della rete, ossia la *data protection* e con essa la tutela da accordarsi al meta-principio dell'identità e della dignità personale che permea l'ordinamento europeo. Nella seconda parte del lavoro verranno quindi analizzati gli ostacoli che a livello geopolitico si frappongono alla realizzazione di una data governance globale costituzionalmente informata. Dall'analisi dell'impianto generale del GDPR, oltre alle generali limitazioni nella tutela del «diritto all'identità personale» tanto a livello micro, quanto a livello macro (gestione dei big-data), emerge infatti come l' assenza di una politica estera comune in materia di monetizzazione e uso dei dati, renda di difficile interpretazione concetti quali «sicurezza nazionale» e «interesse geopolitico» che legittimano la deroga al quadro regolatorio europeo, permettendo ai singoli Stati la condivisione di dati con Paesi terzi tramite accordi bilaterali, anche quando, come nel caso statunitense, obiettivi e standard in materia di *data-protection* appaiono incompatibili con l'approccio dell'Unione. In conclusione, si metterà in luce come il *framework* del costituzionalismo digitale, resti non soltanto fattore di legittimazione della sovranità digitale che in esso trova fondamento, ma anche griglia ermeneutica per valutare, nell'ambito dell'autonomia strategica degli Stati membri nell'applicazione o disapplicazione del regolamento (c.d. *free riding*), cosa possa rientrare nell'alveo della legittima contestazione politica e cosa invece, sfidando il fulcro dell' identità internazionale europea, sia inquadrabile nella cornice della de- europeizzazione.

Abstract. The ability of individual states to autonomously craft regulations concerning the digital economy, oversee strategic infrastructure, manage cybersecurity, and combat misinformation represents a pivotal existential challenge for democratic systems. Following a brief overview of the salient features of so-called digital constitutionalism, the frame in which the European normative turn towards «digital sovereignty» is embedded and interpreted, a focused analysis will delve into the cross-cutting issue preceding any network regulation attempt: the geopolitical barriers to achieving constitutionally informed global data governance. In the second part of the work, the geopolitical obstacles to the realization of a constitutionally informed global data governance will be analyzed. An examination of the GDPR framework highlights not only the general limitations in protecting the «right to personal identity» at both micro and macro levels (in the context of handling big data) but also underscores the challenges in interpreting concepts such as «national security» and «geopolitical interest». These concepts allow exceptions to the European regulatory framework, enabling states to share data with third countries, even when their data protection objectives and standards, as observed in the case of the United States, are not aligned with the EU approach. Finally, the study illuminates how the digital constitutionalism framework not only legitimizes the underlying digital sovereignty but also serves as a hermeneutic tool to discern what falls within legitimate political contestation and what, by challenging the essence of European international identity, can be categorized within the context of de-Europeanization.

Parole chiave. Sovranità digitale – costituzionalismo digitale – data governance – geopolitica dei *big data* – Identità europea transnazionale.

Key words. Digital sovereignty – digital constitutionalism – data governance – geopolitics of big data – Transnational European identity.

.