Dual use by design: identità europea e identità personale al vaglio dei big data.

Isabella de Vivo*

Sommario: 1. Premessa. – 2. La rotta europea per una data-governance "costituzionalmente orientata". – 3. L'ontologia dei dati come risorsa naturale. – 4. I dati come asset strategico. – 5. Il GDPR e le "ragioni di sicurezza nazionale". – 6. Riflessioni conclusive.

1. Premessa

Come scongiurare il rischio che l'interazione tra *agency* umana e *agency* artificiale non assuma le forme di una colonizzazione dello spazio che vogliamo costitutivo dell'idea di individuo e di quell' auto-sovranità che si vuole a fondamento delle società democratico-liberali? Come far sì che, al contrario, tale interazione converga verso un arricchimento del potenziale e della soggettività umana? Quale ruolo è chiamato a svolgere il legislatore sovranazionale in questo processo di transizione di soggettività e sovranità?

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[1] di

*Dottoranda, Sapienza Università di Roma.

[1]Facendo riferimento alla nozione generale accettata a livello internazionale, l'ampio e controverso concetto di Intelligenza Artificiale è riconducibile "alla disciplina appartenente all'informatica, che studia i fondamenti teorici, le metodologie e le tecniche che permettono di progettare sistemi digitali (hardware) e di programmi (software) capaci di fornire all'elaboratore elettronico prestazioni che, a un osservatore comune, sembrerebbero di pertinenza esclusiva dell'intelligenza umana", cfr. M. SOMALVICO, F. AMIGONI, V. SCHIAFFONATI, *La grande scienza. Intelligenza artificiale*, in /www.treccani.it/ 2003. Nel corso del lavoro, si farà, tuttavia, riferimento alla definizione normativa attualmente contenuta nell'art. 3.c.1 dell' AI-Act, che, seguendo la proposta dell'OCSE – definisce sistema di IA "un sistema automatizzato progettato per

"datificare[2]" 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, ovvero, di subire indebite limitazioni nell'esercizio di diritti che attengono agli attributi ontologici della persona, costituisce, oggi, una delle più importanti sfide alla resilienza e al fondamento degli istituti democratici.

Come può evincersi dalla stessa definizione di Intelligenza Artificiale data dal legislatore europeo nell'AI-Act[3], "i sistemi automatizzati" funzionano, con diversi livelli di autonomia, generando output (quali previsioni, contenuti, raccomandazioni o decisioni) deducendoli dagli input che ricevono. Questo significa che la loro "autonomia" e "razionalità" non può prescindere da una formazione estensiva e computazionalmente intensiva fatta di grandi set di dati, regole e ricompense predefinite[4]. I sistemi di *machine learning*[5]*, deep*

---

funzionare con diversi livelli di autonomia, che può mostrare capacità di adattamento dopo l'installazione e che, per obiettivi espliciti o impliciti, deduce, dagli input che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali".

[2] Nel senso "costitutivo del termine": quella che Rouvroy definisce "*algorithmic governmentality*", riferibile in generale ai sistemi automatizzati, consiste infatti nella capacità di "creare" realtà nella stessa misura e nel momento in cui la registrano datificando le relazioni; la datificazione quindi di per sé non è mai passiva né semplicemente "dichiarativa". cfr. A. ROUVROY, T. BERNS, E. LIBBRECHT, *Algorithmic governmentality and prospects of emancipation,* in «Réseaux», I, 177, 2013.

[3]Cfr. nota *supra*.

[4] In merito si veda *ex multis* K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'IA,* Il Mulino, 2021.

[5] Con sistemi di *machine learning* in generale indicheremo il sottoinsieme dell'IA costituito da quella particolare categoria di algoritmi la cui funzione è creare altri algoritmi. Tramite l'analisi dei dati, il riconoscimento delle loro caratteristiche (*pattern*) e l'apprendimento a partire dal loro esame (relazioni di dati), la macchina costruisce induttivamente un modello basato su campioni prendendo in questo modo decisioni operative in quegli ambiti e applicazioni pratiche in cui progettare e programmare algoritmi espliciti risulta impraticabile.

learning e neural learning[6], funzionano attraverso l'elaborazione di enormi quantità di dati che possono essere tanto di "natura personale", tanto "non personale[7]" e allo stesso tempo, sulla base di quest'elaborazione, producono, quale output, nuovi dati e informazioni, in grado influenzare ambienti fisici o virtuali.

La computazione e l'estrazione massiva di dati, di qualsiasi natura essi siano, è dunque il motore di alimentazione imprescindibile per lo sviluppo e l'implementazione di tali sistemi. Ne consegue che i problemi etico-giuridici derivanti dalla applicazione dei sistemi di IA sono inestricabilmente connessi a quelli che attengono i processi di datificazione che essi presuppongono. Problemi, questi, che riguardano tanto il fondamento e la legittimità dell'estrazione dei dati in un ecosistema in cui, come avremo modo di argomentare, la dicotomia oppositiva che distingue tra dati personali e dati non personali rischia di non essere più conferente[8], quanto alle conseguenze sulla tutela dei

---

[6] Di cui i modelli "t*ransformer*" costituiscono un ormai diffuso sottotipo, poiché sono quelli su cui si basano i *Large Lenguage Model* (LLM) come ChatGPT.

[7] Sui limiti di tale bipartizione si veda nota successiva e *infra.*

[8] Come vedremo la c.d. "governance algoritmica" crea doppi statistici ossia combinazioni di correlazioni automaticamente attraverso i big data costituiti e raccolti di default. (cfr. A. ROUVROY, T. BERNS, E. LIBBRECHT, *op. cit.* p.4). I dati restano quindi anonimi, ma è il significato del loro anonimato che è diventato relativo. Ciò non significa che queste informazioni siano "rubate", il che permetterebbe al soggetto di opporvisi, si tratta, infatti, di dati apparentemente innocui, in quanto non in grado di identificare e dunque tecnicamente (e giuridicamente) non personali. La cessione di queste "tracce" non è quindi deliberata, né necessita di consenso; ciononostante il loro trattamento è in grado di incidere direttamente ed indirettamente sulla sfera personale sociale e giuridica dell'interessato, influenzando gli output dei sistemi automatizzati con cui egli entra in relazione. Più utile, allora, sarebbe distinguere tra macro-categorie di dati ed in particolare tra 1) *Volunteer data:* dati forniti volontariamente dagli utenti o dati di identificazione: 2) *Observed data:* dati acquisiti registrando le attività degli utenti; 3*) Inferred data*: dati dedotti dall'elaborazione delle precedenti categorie di dati; cfr. A. PENTANI, D.L. SHIRER, T. HARDON, I.W. BERGER, *Trusted Data: A New Framework for Identity and Data Sharing*, Cambridge, 2019. Il loro utilizzo trascende, come vedremo, la personalizzazione ed il

diritti fondamentali dei potenziali *bias* insiti nei processi di apprendimento e che possono incidere tanto sulla fase di raccolta dei dati (c.d. *observational biases* o "distorsioni di misurazione"), quanto sulla fase di elaborazione e "significazione" degli stessi, nella forme di distorsioni pre-esistenti (*pre-existing bias*) o emergenti (*emergent biases*)[9] .

---

microtargeting a scopi meramente commerciali, manipolativi o politici (aspetti questi ultimi, resi universalmente noti dallo scandalo *Cambridge Analytica*, (su cui si veda *infra)* essendo altresì necessari all'addestramento e lo sviluppo dei sistemi dell'IA a scopi militari.

[9] Nel campo dell'IA, il termine *bias* tende a riferirsi generalmente agli effetti di un sistema informatico, "che discrimina ingiustamente negando un'opportunità, un bene o assegna un risultato indesiderato a un individuo o a un gruppo per ragioni inappropriate, favorendo sistematicamente e ingiustamente alcuni individui o gruppi rispetto ad altri". (B. FRIEDMAN, H. NISSENBAUM, *Bias in Computer Systemsm* in «ACM Transactions on Information Systems», XIV, n. 3, 1996, pp. 330-347). In particolare i c.d. *Observational bias,* o bias di misurazione, sono legati alla raccolta dei dati poi utilizzati nel training della macchina. È il caso in cui l'algoritmo predittivo è costruito su un set di dati che è già in partenza discriminatorio. Dinanzi ad un input "biased" anche l'output sarà "biased". Con il termine *pre-existing-biases*, si fa riferimento a possibili distorsioni del processo decisionale o valutativo determinate da "pregiudizi" insiti all'interno di tali strumenti tecnologici. I c.d. pregiudizi o distorsioni emergenti (*emergent biases),* sorgono, invece, durante i successivi stadi di apprendimento e questo avviene nonostante l'apparente neutralità iniziale dei parametri di addestramento. Si rivelano pertanto estremamente difficili, se non impossibili, da prevedere in fase di progettazione. I possibili effetti discriminatori degli output, c.d. *proxy discriminations* (cfr. F.Z. BORGESIUS, *Discrimination, Artificial Intelligence and Algorithmic Decision-Makin*g, Anti-discrimination Department, Council of Europe, Strasbourg 2018; A.E.R. PRINCE, D. SCHWARCZ, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, in «Iowa L. Rev». 105, n. 3, 2020) in questo caso sorgono, allora, quale conseguenza involontaria delle correlazioni statistiche del sistema e a loro volta possono essere soggette a meccanismi di amplificazione circolare e progressiva (*feedback loops*). Per una trattazione più ampia e approfondita del tema sia consentito rimandare a I. DE VIVO, *La ricerca di un modello per la regolare le nuove tecnologie*, in *Diritto di Internet e dei Social Media,* a cura di E. BUCALO, M. CAPORALE, A. STERPA, Editoriale Scientifica, Napoli 2024a. pp. 79-

Se democrazia e tutela dei diritti fondamentali ed *in primis* "il diritto all'identità personale[10]," che il libero agire presuppone, sono indissolubilmente legati, per comprendere la natura dell'impatto dei sistemi di IA su individui e società, una previa riflessione sullo statuto ontologico, prima ancora che giuridico, da accordare ai dati -risorsa base della computazione- e quindi sul loro valore sociale, politico, ed ideologico, oltre che economico, è la premessa indispensabile a qualsiasi tentativo di regolazione efficace. Da un lato, infatti, si tratta di comprendere l'impatto strutturale dei processi di datificazione sulla garanzia dei diritti sanciti dalla Carta Europea dei Diritti Fondamentali, e in particolare sul principio dell'identità personale, dall'altro, analizzare il contesto geopolitico entro cui si gioca la sfida Europea per la costruzione di una data governance coerente con il proprio assetto valoriale. Un contesto che, come vedremo, in apparente opposizione al processo di globalizzazione, vede la tendenza centripeta alla progressiva territorializzazione e ri-centralizzazione del controllo sui flussi di dati da parte degli Stati per "ragioni di sicurezza nazionale"[11].

Al fine, dunque, di inquadrare il progetto europeo per una "sovranità digitale costituzionalmente orientata" e gli ostacoli che, attualmente, sembrano frapporsi alla sua realizzazione, si procederà, in via preliminare, ad analizzare criticamente l'ontologia alla base del "capitalismo computazionale"[12] che legittima la visione dei dati come

---

102.

[10] Sulla necessità di riformulare il diritto alla privacy come il diritto all'identità personale, ovvero alla libertà di costruzione (o co-costruzione) e sviluppo della nostra identità personale si vedano: S. ESKENS, *The fundamental rights of news users: The legal groundwork for a personalised online news environment*, Research output: PhD-Thesis – Research and graduation external, 2021; S.O. SØE, J.E. MAI, *Data identity: privacy and the construction of self*, in «Synthese», CC, n. 6, 2022, pp. 492 e ss.; E.M. RENIERIS, *Beyond data: reclaiming human rights at the dawn of the metaverse*, Cambridge 2023; da ultimo S. TIRIBELLI, *Identità personale e algoritmi, Una questione di filosofia* morale, Roma 2023.

[11] Sui precessi di decentralizzazione e ricentralizzazione si veda D. LAMBACH, T*he territorialization of cyberspace*, in «International Studies Review» XXII, n. 3, 2020.

[12] B. STIEGLER, *La società automatica 1. L'avvenire del lavoro,* Meltemi, Milano 2019. Anche detto "capitalismo informazionale" (J. COHEN, *Between Truth and Power: the Legal Constructions of Informational*

"risorsa naturale" o "materia prima" liberamente disponibile all'appropriazione e alla conseguente mercificazione; successivamente l'analisi si concentrerà su l'ulteriore cruciale aspetto, destinato inevitabilmente ad incidere sul disegno europeo per una data governance globale, ossia la valenza geo-strategica dei dati, quale risorsa indispensabile allo sviluppo dell'IA anche in campo bellico. Se, come si argomenterà, i dati rappresentano a tutti gli effetti un asset strategico per la sicurezza nazionale, la capacità dell'Europa di esercitare il suo potere normativo sarà allora limitata, *in primis* a livello interno, dalla competenza esclusiva riservata agli Stati Membri in materia.

2. La rotta europea per una *data-governance* "costituzionalmente orientata".

Non è un caso che sul tema della *data governance* convergano gli attuali sforzi normativi dell'UE (dal GDPR al lancio da parte della Commissione della Strategia per il Mercato Unico dei Dati 2020) per la costruzione della c.d. "sovranità digitale europea[13]", intesa, secondo

---

Capitalism, Oxford University Press, 2019), "*platform capitalism"* (N. SRNICEK, *Platform capitalism, Polity* Press, Cambridge, UK 2016) o "*big data capitalism"* (CH. FUCHS, *Karl Marx in the Age of Big Data Capitalism. Digital Objects, in Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*, a cura di D. CHANDLER, CH. FUCHS (Eds.) University of Westminster Press, London 2019). In letteratura si veda anche N. COULDRY, U.A. MEJIAS, *The costs of connection: How data is colonising human life and appropriating it for capitalism,* Stanford University Press, 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», XXVII, n. 2, 2023, pp. 333–349.

[13] Il presidente della Commissione europea 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/ sull'importanza di investire sulla "*nostra sovranità tecnologica"* cfr. U. Von Der Leyen, *A Union That Strives For More: My Agenda for Europe,* in *Political Guidelines for the Next European Commission 2019-2024*, 2019, https://ec.europa.eu/.

le dichiarazioni ufficiali e i regolamenti emanati, quale *obiettivo strumentale* all'affermazione di un'identità normativo-valoriale in linea con le radici etiche e costituzionali dell'Unione[14].

Tale strumentalità e funzionalizzazione alla tutela dei diritti fondamentali individuali (nucleo duro del pur dibattuto concetto di identità costituzionale europea[15]) è un attributo chiave per

[14] 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 e l'AI-Act.

[15]Il concetto di identità costituzionale è un'operazione interpretativa, si basa dunque non su disposizioni (l'atto formale), ma su norme (i.e. il contenuto che ne deriva). Trattandosi del prodotto dell'interpretazione può prescindere dall'esistenza di un testo scritto come accade appunto in Europa. Ciò nonostante, si ricorda che la CDFUE è parte integrante del trattato di Lisbona, quindi dotata della stessa efficacia sugli ordinamenti nazionali del Trattato cui inerisce. Ai sensi dell'Articolo 6 (ex articolo 6 del TUE) p.(1) "la Carta dei diritti fondamentali dell'Unione, ha lo stesso valore giuridico dei trattati". Lo stesso può dirsi della CEDU, in ragione del principio della "massimizzazione della tutela" codificato all'art. 53 della Carta. La Carta richiede, infatti, di essere intesa alla luce della CEDU, fornendo, quindi, anche un criterio interpretativo orientato appunto al principio "della maggior tutela". In merito si veda A. RUGGERI, *La Carta di Nizza-Strasburgo nel sistema costituzionale europeo*, in «Rivista AIC», 3/2020a. p. 135. La ricerca del massimo standard di protezione per i diritti (e, in genere, degli interessi costituzionalmente protetti) costituisce, del resto, come sostenuto dall'A. un autentico "meta-principio", *ibidem*. Si veda anche ID. *Tecniche decisorie dei giudici e "forza normativa" della Carta di Nizza-Strasburgo*, in «Forum di Quad. cost.» 2020b; A. RANDAZZO, *Il "metaprincipio" della massimizzazione della tutela dei diritti*, in «Dir. fond.» (www.dirittifondamentali.it), 2, 2020, pp. 689 e ss; I. ANRÒ, *Carta dei diritti fondamentali dell'Unione europea e CEDU: dieci anni di convivenza*, in «Federalismi», 19, 2020 pp. 109 e ss. In Italia, sul valore "tipicamente costituzionale" ha riconosciuto" alla Carta

comprendere l'idea di sovranità dalla prospettiva dell'Unione. Il concetto di sovranità è infatti utilizzato in diversi ambiti politici ed economici, dai Paesi più centralizzati e autoritari alle democrazie liberali ed ha acquisito, pertanto, una vasta varietà di connotazioni, declinazioni e attributi. Se, tuttavia, il suo significato specifico varia in base ai diversi contesti nazionali e agli accordi degli attori è, soprattutto, in base all'idea e al tipo di *autodeterminazione* che questi attori enfatizzano[16] (*i.e.* autodeterminazione dello Stato, delle autorità private o degli individui), che può tracciarsi un *discrimen* significativo. Muovendosi nel solco del principio dell'autodeterminazione individuale, la strategia europea, sembra problematizzare l 'attuale configurazione della trasformazione digitale non solo come una minaccia allo "Stato sovrano" – quanto esplicitamente al "soggetto sovrano[17]". Sulla linea tracciata dal GDPR il principio dell'auto-determinazione del *data subject,* è allora, in primis, strumentale all'idea della sovranità digitale dell'utente[18]". È qui che risiede, dunque, la peculiarità del progetto europeo, in cui il concetto di "sovranità digitale individuale" assurge a chiave ermeneutica e presupposto di legittimazione delle rivendicazioni sovranazionali. La sovranità digitale può essere allora compresa come "la somma di tutte le capacità e le possibilità di individui e istituzioni di essere in grado di esercitare

---

dell'Unione e, in conseguenza, anche alla CEDU si veda Corte Cost., sent. n. 269 del 2017.

[16] Si vedano J. POHLE, T. THIEL, *Digital sovereignty, in «Internet Policy Review»*, 9(4), 2020.

[17] Cfr. J. WINKLER, F. DAMMANN, *Digitally Competent – Digitally Sovereign – Digitally Civic: geopolitics of Subject Formation in the German Context*, 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 (eds) *Contested Spatialities of Digital Sovereignty,* a cura di, 2022, pp. 924-928. Si vedano anche J. POHLE, *Digital sovereignty – a new key concept of digital policy in Germany and Europe*, Konrad-Adenauer-Stiftung, Berlin 2020 e L. FLORIDI, *The fight for digital sovereignty: what it is, and why it matters, especially for the EU,* in «Philosophy and Technology» XXXIII, n.3, 2020. pp. 369-378.

[18] Cfr. T. CHRISTAKIS, '*European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy*, in «SSRN Electronic Journal», 2020, p.18, trad. nostra.

il proprio ruolo nel mondo digitale in modo indipendente, autodeterminato e sicuro"[19].

Distanziandosi, quindi, da approcci sovranisti di stampo stato-centrico rinvenibili tanto in regimi autoritari, quanto in quelle democrazie liberali che mirano alla "sovranità informativa nazionale", la strategia europea per la sovranità si pone come "come terza opzione" nelle attuali battaglie geopolitiche e geoeconomiche globali per i profitti della trasformazione digitale[20]. Se le strategie di chiusura sono inevitabilmente in tensione con i processi di interconnessione globale, diverso è il discorso quando la sovranità digitale, come emerge *dalle priorità della Commissione europea per il periodo 2019-2024*[21], è utilizzata per legittimare strategie di applicazione di standard tecnologici e/o normativi con un impatto potenzialmente globale.

Il nuovo quadro regolatorio che ne emerge è da leggersi in continuità con quello che viene definito "costituzionalismo digitale"[22], ossia quel processo di "democratizzazione autopoietica della rete"[23]

---

[19] Cfr. Centro di competenza tedesco per l'informatica pubblica (KZIT) (2017: 3).

[20] Cfr. T. CHRISTAKIS, *op. cit.*

[21] Cfr. P. HUMMEL, M. BRAUN, M. TRETTER, P. DABROCK, *Data sovereignty: A review*, in «Big Data & Society», VIII n. 1, 2021.

[22] Il termine "costituzionalismo digitale" reso popolare dal report di ricerca del *Berkman Center for Internet and Society* dell'Università di Harvard definisce la "costellazione di iniziative che hanno provato ad articolare un insieme di diritti politici, norme di governance, e limitazioni all'esercizio del potere su Internet". Sul tema si veda anche E. CELESTE, *Digital Constitutionalism: A New Systematic Theorization,* In «International Review Of Law, Computers & Technology», XXXIII, 1, 2019, pp. 88 e ss.; C. PADOVANI, M. SANTANIELLO, *Digital Constitutionalism: Fundamental Rights and Power Limitation in the Internet Eco-System,* in «International Communication Gazette», LXXX, n. 4, 2018, pp. 295-301.

[23]L'autopoiesi, dal greco αὐτός (autós) "se stesso" o "da sé" e ποιεῖν (poieín) "creare" o "produrre", dunque, letteralmente "autocrearsi", è quello che è accaduto nella rete attraverso la proclamazione spontanea di principi e diritti volti a democratizzare l'ecosistema digitale, sulla spinta di soggetti che operano al di fuori di un contesto strettamente politico, come le organizzazioni non governative e le comunità epistemiche. Si tratta dunque di una forma di costituzionalismo spontaneo, c.d. "sociale", su cui non può che rimandarsi a G. TEUBNER, *Societal Constitutionalism;*

che il nuovo corpus regolamentare (*Digital Services Package*) mira ad abilitare "proceduralmente" al fine di rendere effettiva la protezione dei diritti fondamentali al di là dei confini territoriali[24].

Vi è tuttavia un *discrimen* importante rispetto alle forme di costituzionalismo pre-digitale: se quest'ultime hanno storicamente affrontato e limitato l'esercizio del potere da parte dello Stato nazionale a tutela dei diritti individuali, nel mutato contesto geopolitico lo sforzo è volto ad arginare, da un lato, il potere politico di nuovi "attori ibridi[25]", in grado di limitare prerogative tipicamente statuali quali il

---

Alternatives to State-Centred Constitutional Theory? in C. JOERGES, I.J. SAND, G. TEUBNER (eds) *Transnational Governance and Constitutionalism. International Studies in the Theory of Private Law*, Hart 2004; ID. G. TEUBNER, *Constitutional Fragments: Societal Constitutionalism and Globalization*, Oxford University Press 2012; A.JR. GOLIA, G. TEUBNER, *Societal Constitutionalism: Background, Theory, Debates,* in «ICL Journal» XV, n. 4, 2021, pp. 357-411.

[24] Sul progetto di sovranità europea quale terzo modello nella governance di Internet mosso dal tentativo di democratizzare e "costituzionalizzare" Internet, cfr. G. DE GREGORIO, *The Rise of Digital Constitutionalism in the European Union,* in «International Journal of Constitutional Law», XIX n.1, 2020, pp. 41-70. Si veda anche M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance,* in «Rivista italiana di informatica e diritto», IV, n.1, 5-5, 2022. 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.

[25] Sul tema la letteratura è amplissima, si veda almeno N. HELBERGER, *The political power of platforms: How current attempts to regulate misinformation amplify opinion power* in «Digital Journalism», VIII, n. 6, 2020, pp. 842-854; O. POLLICINO, *L'efficacia orizzontale dei diritti fondamentali previsti dalla Carta. La giurisprudenza della Corte di giustizia in materia di digital privacy come osservatorio privilegiato*, in «MediaLaws», n. 3, 2018, pp. 138-163; ID. O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?,* Hart Publishing, 2021; 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», III, n. 2, 2021, pp. 43-64 E. CELESTE, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. FABBRINI, E. CELESTE, J. QUINN

bilanciamento dei diritti fondamentali dall'altro, forme di colonialismo culturale derivanti dall'imposizione surrettizia di assetti valoriali e obiettivi strategici difficilmente compatibili con le prerogative dell'Unione. Il riferimento, come si argomenterà, va in particolare alla diversità di obiettivi che animano il progetto europeo di sovranità ed il tentativo da parte degli USA di nazionalizzazione dei dati tramite il controllo tanto dei flussi informativi estratti sul proprio territorio, quanto di quelli estratti negli spazi delle "colonie digitali[26]" a scopi di supremazia geostrategica [27]. Tale patto tecnocratico tra poteri pubblici

(eds) *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Hart, 2021. Sull'inquadramento delle piattaforme come "poteri privati" cioè, soggetti che agiscono nelle forme del diritto privato, ma che, per la loro posizione di forza economica e/o sociale, sono capaci di incidere sull'esercizio delle libertà fondamentali dei singoli, si veda anche O. GRANDINETTI, *Le piattaforme digitali come "poteri privati" e la censura online,* in «Rivista italiana di informatica e diritto» IV, n.1, 2022, pp. 175-188; M. BETZU, *Poteri pubblici e poteri privati nel mondo digitale*, in «GruppodiPisa», n. 2, 2021.

[26] Il discorso della sovranità è strettamente collegato a quello dell'autonomia tecnologica e quindi, soprattutto, alle preoccupazioni per la dipendenza dell'Europa dalle big-tech statunitensi; preoccupazioni queste particolarmente sentite in Germania ed in Francia. Si veda a titolo esemplificativo, il rapporto del Senato francese (*Office parlementaire d'évaluation des choix scientifiques et technologiques)*, pubblicato nel 2017 e incentrato sull'IA, che considera "la colonizzazione digitale americana una realtà indiscutibile". Cfr. C. DE GANAY, D. GILLOT, *Pour une intelligence artificielle maîtrisée, utile et démystifiée, Rapport*, Office parlementaire d'évaluation des choix scientifiques et technologiques, n. 464, March, 15, 2017, at.24. Per citare le parole di Pierre Manière: "la Francia è diventata il vassallo di un 'cyber-impero', quello degli Stati Uniti e dei suoi giganti di Internet. [...] L'Europa ha scelto la subordinazione, la provincializzazione e la colonizzazione nei confronti degli Stati Uniti. [...] È diventata la 'dispensa' digitale dell'America. [...] La sovranità digitale è importante quanto la sovranità nucleare. Senza questo controllo, saremmo diventati una nazione sotto tutela", P. MANIÈRE, *L'Europe, "garde-manger" numérique des États-Unis,* in "La Tribune", January 14, 2020.

[27]. Tale strategia ha come necessarie controparti i big players del digitale (la c.d. GAFAM: Google, Apple, Facebook, Amazon, Microsoft) che hanno appunto base statunitense, quali *longa manus* nell'approvvigionamento dei dati. In merito si veda Simitis, il quale rileva

e privati "uniti per la sorveglianza" trova legittimazione in una narrazione che - coadiuvata da una atmosfera di normalizzazione efficacemente descritta in letteratura come "realismo della sorveglianza"[28] - vede le ragioni di sicurezza nazionale a priori prevalenti sulla tutela dei diritti individuali e che ben si presta a strumentalizzazioni a livello politico volte a giustificare limitazioni anche estreme della libertà personale, in contrasto con l'assetto valoriale europeo.

Come detto, per cercare di comprendere appieno gli obiettivi della "terza opzione europea", ma anche gli ostacoli che, a livello non soltanto internazionale, ma anche regionale, attualmente si frappongono alla sua realizzazione, è necessario in primis disambiguare il concetto di "dato", tenendo conto della natura bifronte di quella che viene comunemente definita la "materia prima" della *data economy*. È con l'intrinseca valenza duale dei dati che la sovranità digitale e "l'autonomia strategica[29]", concepita come generale capacità

---

come il governo americano «non si attenga più alla tradizionale raccolta diretta di dati, ma si rivolga ad 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; cfr, S. SIMITIS, (2003), *Privacy- An Endless Debate?* In «California Law Review», XCVIII, n. 6, 2010, pp. 1989-2005. 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*, Public Affairs, New York 2019.

[28] Cfr. L. DENCIK, *Surveillance realism and the politics of imagination: Is there no alternative?,* in «Krisis. Journal for Contemporary Philosophy», n.1, 2018.

[29] 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. Di 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*

di salvaguardare gli interessi e i valori della società europea, sono chiamate a confrontarsi.

Le operazioni di sorveglianza e di *data mining*[30] vengono, infatti, solitamente intese da un punto di vista strettamente commerciale concentrandosi in particolare sui dati estratti dalle grandi piattaforme a scopo pubblicitario[31]. La raccolta pervasiva di dati, presupposto

"strategie in autonomia"? in «Le istituzioni del federalismo», I, n. 2, 2022, pp. 45-64; S. POLI, E. FAHEY, *The strengthening of the European technological sovereignty and its legal bases in the Treaties*, in «rivista.eurojus.it», 2022.

[30] *Il data mining* o "*automatic crossreferencing of hereogeneus data"* è il processo di esplorazione e analisi di enormi volumi di dati detenuti da grandi organizzazioni, governi e colossi tecnologici (il riferimento va in particolare all'oligopolio pentagonale costituito dalla c.d. GAFAM (*cit.)* negli USA e alla c.d. BATX: (Baidu, Alibaba, Tencent, Xiaomi, in Cina) al preciso scopo di scoprire pattern nascosti, relazioni all'interno dei dati, trend e altre informazioni significative. Set di dati (personali e non) 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).

[31] Volendo fornire un quadro orientativo dei principali settori in cui il data mining (sulla cui definizione si rimanda *supra*) 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 e Social Media: analisi dei sentimenti, monitoraggio delle tendenze; determinazione dei comportamenti di consumo informativo tramite algoritmi di raccomandazione (RS) e di personalizzazione dei contenuti (*soft moderaton*); moderazione e filtraggio dei contenuti nocivi/illeciti (*hard moderation*); 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

ontologico dello sviluppo dell'IA, sta, tuttavia, trasformando le vulnerabilità individuali e commerciali anche in potenziali debolezze inerenti alla sicurezza nazionale. Di conseguenza, i dibattiti politici e accademici sui flussi di dati, in particolare a seguito delle rivelazioni Snowden[32], sono diventati sempre più "*securitizzati*, territorializzati e, in ultima analisi, geopoliticizzati[33]".

Nella seconda parte di questo contributo, si cercherà, dunque, di mettere in luce, come nell'attuale geopolitica del capitalismo informazionale[34], i dati raccolti su un determinato territorio, o meglio dalle popolazioni che lo abitano, non rappresentino soltanto remunerazione per il capitale, ma anche plusvalore di potere statale in termini di autonomia geo-strategica e sicurezza e come questo si rifletta sui limiti e sull'efficacia della regolazione sovranazionale a livello tanto regionale quanto globale. La capacità dell'Europa di esercitare il potere normativo in materia, sarà infatti limitato dalla competenza esclusiva degli Stati membri sulle questioni riguardanti la sicurezza nazionale che, come noto, restano di "esclusiva responsabilità di ciascuno Stato membro[35]".

---

settore civile non esaurisce l'ambito di sviluppo e applicazione delle tecniche di data mining; su questo aspetto si veda A. ARESU, *Le potenze del capitalismo politico. Stati Uniti e Cina*, La Nave di Teseo, 2020.

[32] 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. In merito, non può che rimandarsi all'autobiografia di Snowden: E. SNOWDEN, *Errore di sistema,* Longanesi, 2019. Per approfondimenti si veda anche S. LANDAU, *Making Sense from Snowden: what's significant in the NSA surveillance revelations,* in «IEEE Security & Privacy», XI, n. 4, 2013, pp. 54-63 e A. WIENER, *Uncanny Valley: Seduction and Disillusion in San Francisco' Startup Scene,* London 2020, p. 127.

[33] D. LAMBACH, *The territorialization of cyberspace,* cit. p.15.

[34] Sulle varie definizioni del capitalismo digitale sorte in letteratura, si veda *supra* nota 13.

[35] Cfr. art.4(2) TUE.

3. L'ontologia dei dati come risorsa naturale.

Siamo abituati a sentir parlare di dati, in particolare di *raw data* (dati grezzi) come "materia prima" della *data economy* e intenderla dunque, al pari di ogni altra risorsa naturale, come preesistente a qualsiasi attività umana, 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)[36] secondo cui «*I dati sono l'equivalente del 21° secolo di una risorsa naturale globale, come il legname, il ferro o il petrolio*[..]».

Una narrazione questa che, tuttavia, oltre ad essere epistemologicamente fuorviante, rischia di oscurare i presupposti ideologici alla base della quantificazione del sociale[37].

---

[36] 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. 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. Ha viaggiato globalmente nel 2016 per cercare idee innovative dai soggetti coinvolti nelle operazioni militari per migliorare i processi utilizzati in tutti i teatri operativi. Joshua Marcuse ed Eric Schmidt ne sono stati rispettivamente il primo Direttore Esecutivo e il primo Presidente. L'organizzazione consiglia il Dipartimento della Difesa in aree chiave come l'IA e la modernizzazione digitale.

[37] Utilizziamo il termine quantificazione, come sinonimo di datificazione. Quest'ultima altro non è, infatti, se non la trasformazione dell'azione sociale in dati quantificati online, che diventa così tracciabile in tempo reale e soggetta ad analisi predittiva. Le aziende e le agenzie governative scavano nelle pile in crescita esponenziale di metadati raccolti attraverso piattaforme di social media e di comunicazione, come Facebook, Twitter, LinkedIn, Tumblr, iTunes, Skype, WhatsApp, YouTube e servizi di posta elettronica gratuita, per tracciare informazioni sul comportamento umano: "Ora possiamo raccogliere informazioni che prima non potevamo, siano esse relazioni rivelate dalle telefonate o sentimenti svelati attraverso i tweet"; cfr. V.M. MAYER-SCHOENBERGER, K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, John Murray Publishers Ltd, 2013.

Questa visione, che induce a considerare la raccolta come semplicemente naturale ed "automatica", facilita, infatti, un immaginario di trasformazione sociale *data-driven* che fa poco o nessun riferimento al prezzo che le persone potrebbero pagare per la loro connettività, o meglio lo "normalizza" oscurando le implicazioni etiche della datificazione quale strumento di potere esercitato attraverso pratiche di framing su popolazioni e o gruppi mirati (con gli evidenti rischi di discriminazione ad esse connessi[38]) e quale atto unilaterale di formazione della soggettività.

Presupposto epistemologico implicito è la presunta oggettività dei big data per cui sarebbero gli stessi dati, senza alcuna pregiudiziale e senza essere condizionati dall'orizzonte di attese dell'osservatore, a dirci del benchmark, del modello e della correlazione significativa fra un numero tendenzialmente infinito di variabili. Così argomentando, la "conoscenza" prodotta sembra emergere direttamente dai big data, una conoscenza che, dunque, pre-esiste a qualsiasi ipotesi: le ipotesi stesse sono "generate" dai dati, liberando così dalla necessità di elaborare o lasciar sopravvivere qualsivoglia teoria[39].

---

[38] Con il termine "dataismo" Josè Van Dijk descrive la componente ideologica della datificazione, ossia la normalizzazione del *data-sharing*: la cessione dei propri dati è l'ineludibile prezzo da pagare per i servizi dell'informazione e per la sicurezza. J. VAN DIJK, *Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology,* in «Surveillance & Society», XII, n. 2, 2014, pp. 197–208. In questo modo la *datificazione* è diventato, infatti, lo strumento legittimo ed inevitabile per accedere studiare e monitorare in modo pervasivo e capillare il comportamento delle persone, pur basandosi su presupposti ontologici ed epistemologici problematici.

[39] Così CH. ANDERSON, *The End of Theory: the Data Deluge Makes the Scientific Method Obsolete*, in "Wired", 2008. Si tratta di un assunto, tuttavia, ampiamente decostruito in tutti i campi della scienza; anche l'apprendimento statistico che deriva dalla potenza dei big data non può essere considerato, infatti, come chiave euristica da sola sufficiente alla comprensione della realtà fenomenica e sociale; prescindere da ogni nesso causale, significherebbe, se non altro, accettazione fideistica della verità algoritmica; si veda *ex multis*: R. KITCHIN, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, Sage, London 2014; J. VAN DIJCK, *Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology* cit.; J. YU, N. COULDRY,

Tuttavia, 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 (interpretazione) e successiva appropriazione[40]. Parlare di "materia prima" prodotta astraendo e riducendo il mondo in forme rappresentative e definirla "*raw data*" equivale a sostenere un ossimoro[41]. Se questo significa da un lato che i dati, essendo un derivato dell'interpretazione, non sono in grado di "parlare da soli[42]", liberi da pregiudizi umani, posizionamenti o inquadramenti predeterminati, dall'altro indica che la materia prima, oggetto di estrazione di conoscenza, risiede in qualcosa di diverso.

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: tale "risorsa prima" è rappresentata dalle relazioni umane in quanto tali, che tradotte in forma *data relations*[43] sono strutturate per la mercificazione sul mercato primario e secondario dei dati. Si tratta, dunque, dell'esistenza umana in quanto tale, che - colta in ogni singolo aspetto individuale e relazionale - nella dimensione dell'*onlife*[44] diventa suscettibile di quantificazione e successiva appropriazione[45]. Se così è, oggetto di quella che viene definita "governance

---

Education as a domain of natural data extraction: analysing corporate discourse about educational tracking, in «Information, Communication & Society», XXV, n.1, 2022.

[40] R. KITCHIN, *Thinking critically about and researching algorithms,* in «Information, Communication & Society», XX, n.1, pp. 1-16, 2019.

[41] "*Raw data" is both an oxymoron and a bad idea*", così G.C. BOWKER, *Memory Practices in the Sciences*, MIT Press, 2008. citato in L. GITELMAN, '*Raw Data' is an Oxymoron*, MIT Press, Cambridge 2013. In merito si veda ancora R. KITCHIN, *Thinking critically about and researching algorithms*, cit.

[42] Cfr.. CH. ANDERSON *op.cit.*

[43] Cfr. N. COULDRY, U.A. MEJIAS, *The costs of connection: How data is colonising human life and appropriating it for capitalism,* cit.

[44] Cfr. L. FLORIDI, La quarta rivoluzione. *Come l'infosfera sta trasformando il mondo*, [2014] Raffaello Cortina Editore, Milano 2017.

[45] Sul tema si veda L. GITELMAN, '*Raw Data' is an Oxymoron*, cit.; D. Beer, *The Social Power of Algorithms*, in «Information, Communication & Society» XX, n. 1, 2017, pp. 1-13.

algoritmica[46]" sono precisamente le relazioni: "i dati condivisi sono relazioni e sussistono solo come relazioni; la conoscenza generata consiste in relazioni di relazioni.[47]"

È chiaro allora 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. Parlando di "privacy informazionale[48]" non è alla "tutela della riservatezza" nel senso analogico del termine a cui si fa riferimento, ma a quello spazio identitario minimo che è garanzia di uno sviluppo che possa dirsi moralmente libero della personalità individuale[49]. In altre parole, se il più contiene il meno, è all'auto-sovranità cognitiva che l'agire libero presuppone a cui deve farsi riferimento e da cui, a sua volta, dipende la resilienza di una sfera pubblica autonoma ed, in ultima analisi, il corretto funzionamento delle istituzioni democratiche.

Shock pubblici, come le conseguenze dello scandalo Cambridge Analytica del 2018[50], hanno, del resto, reso noti i pericoli insiti nella

---

[46] Sul concetto di governance o "governamentalità algoritmica" si veda A. ROUVROY, T. BERNS, E. LIBBRECHT, *op. cit.*

[47] Ivi p.20, ove la parola "relazione" sta ad attestare un'operazione che collega a e b, pur potendo trascurare ciò che si cela dietro i termini così collegati. La forza della "governamentalità algoritmica" (e dell'anonimizzazione dei dati) risiede, infatti, nella sua capacità di astrarre questa relazione, nello stesso modo in cui "è incapace di afferrare il divenire inerente a questa relazionalità".

[48] Cfr. L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo,* cit.

[49] 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, *op. cit*. p.15.

[50] Il caso *Cambridge Analytica,* scoppiato nel 2018, è stato uno dei più grandi scandali relativi alla 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

capacità di elaborazione dei dati sul corretto funzionamento dei processi elettorali e come questi rendano gli individui vulnerabili alla sorveglianza a scopi predittivi (*dataveillance*[51]) e alla manipolazione informazionale intenzionale[52] (profilazione psicografica e *hypernudging*[53]*)*.

---

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

[51] Per "dataveglianza"si intende in particolare la sorveglianza in forma continua attraverso l'uso di (meta)dati cfr. R. RALEY, *Dataveillance and Countervailance,* in 'Raw Data' Is an Oxymoron, *cit.* pp. 121–146; si veda anche J. VAN DIJK, *op.cit.* e D. LYON, *Surveillance culture, ethics and digital citizenship*, in «International Journal of Communication», 11, 2017, pp. 824–842.

[52] Si veda ancora D. BEER, *op.cit.* pp. 1-13; L. GITELMAN, *op. cit.*

[53] i.e. strategia che imposta 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.», XX, n. 1, 2018, pp. 118-136. 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 col "*nudging"* che, come pratica di regolazione comportamentale, non riguarda la creazione e

Il drammatico impatto dei descritti fenomeni distorsivi, ha dato nuovo impulso al dibattito sul tipo e sulla natura degli interventi normativi necessari ed idonei a controbilanciare l'opacità delle forme ibride di controllo sui flussi informativi basate sulla profilazione e la personalizzazione algoritmica[54]. Tuttavia, ciò che ad un sguardo critico non può sfuggire è come la regolamentazione orientata alla moderazione dei contenuti, per quanto cruciale, non sia, da sola, sufficiente a risolvere gli squilibri dell'attuale ecosistema informativo[55]. A dover essere affrontata è in primis la normalizzazione dei presupposti impliciti che rendono possibile la manipolazione degli individui e i relativi effetti sociali, legittimati dal modello aziendale a fondamento del capitalismo della sorveglianza[56].

La cessione delle "tracce" comportamentali (tracce da sole insignificanti, segmentate e decontestualizzate) e dunque tecnicamente (e giuridicamente) non personali non è deliberata, né necessita di consenso è semplicemente normale ossia operata di *default*[57]. Ciò che, tuttavia, resta occulto ed incontrollabile per il "soggetto datificato" è la loro "traiettoria" e quindi la capacità di incidere direttamente e indirettamente sulla sua sfera cognitiva, prima ancora che sociale e giuridica, influenzando gli output dei sistemi automatizzati con cui egli entra in relazione[58]. È importante allora riconoscere nella regolazione

---

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.

[54] L'attuale approccio europeo è per lo più incentrato su interventi di *hard* e *soft-moderation* preventivi e successivi dell' output algoritmico, cfr. *Digital Services Act* (DSA) reg. UE 2022/2065.

[55] Per tali rilievi critici si veda A. JR. 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 si veda D. Nguyen, B. Beijnon, *op. cit.*

[56] Su cui S. ZUBOFF, *op.cit.*

[57] Tali tracce, all'apparenza innocue, in quanto non in grado di identificare, restano al di fuori del perimetro di applicazione del GDPR, così come del più recente Data-Act. La "dataveglianza" come visto opera attraverso metadati, cfr. nota *supra.*

[58] Quando si tratta di intermediazione informativa, i sistemi automatizzati

il valore di tutti quei dati c.d. "esterni" o "scorie digitali" -sottoprodotto dell'interazione uomo-macchina- la cui elaborazione è destinata sul lungo termine a plasmare orizzonti decisionali, cognitivi e percettivi di individui e gruppi sociali, andando direttamente ad impattare il nucleo essenziale di diritti umani quali il diritto al pieno e libero sviluppo della propria personalità.

La costruzione di un'alfabetizzazione mediatica critica (*critical data literacy*[59]*)*, tesa a rendere consapevoli gli utenti del rapporto originario e costitutivo con i dati generati e ceduti, consapevolmente o meno, nell'ecosistema digitale, è allora una 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". È nella tutela di una privacy intesa in senso ampio quale "libertà intellettuale[60]" e diritto al pieno sviluppo della propria personalità che va trovato il fine ultimo della tutela.

4. I dati come asset strategico

Se la raccolta e l'uso dei dati, rappresentano una potenziale minaccia al nucleo essenziale dei diritti individuali, che direttamente e indirettamente incide sulla resilienza e sul 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

---

che di tali tracce si nutrono, agendo e determinando gli orizzonti semantici del soggetto, agiranno su un presupposto fondamentale della costruzione identitaria quale è appunto la libertà epistemica. In merito sia consentito rimandare a I. DE VIVO, *Il sé allo specchio dell'algoritmo. Libertà epistemica e identità individuale*, in A. STERPA, C. CAPASSO A. CORTAZZO, I. DE VIVO, C. LISI, R. MADAIO, S. TIRIBELLI, G. SGUEO N. VICECONTE *(a cura di) L'ordine giuridico dell'algoritmo,* Editoriale Scientifica, Napoli 2023, pp. 24-33.

[59] T.P. NICHOLS, A. SMITH, *Critical literacy, digital platforms, and datafication*, in T.P. NICHOLS, A. SMITH, S. BULFIN, A. STORNAIUOLO (eds) *Handbook of critical literacies*, Routledge 2021

[60] Cfr. S. ESKENS. *op. cit*. Si veda anche N.M. RICHARDS, *Why Privacy Matters: An Introduction*, Oxford Press, Oxford 2021. http://dx.doi.org/10.2139/ssrn.3973131

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[61].

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."

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[62] .

Si tratta di un aspetto fondamentale da tenere in considerazione, per vagliare efficacia e applicabilità a livello regionale e globale del quadro regolamentare europeo in materia di data governance ed in particolare gli ostacoli, che in ossequio al principio di sovranità territoriale, si frappongono alla sua realizzazione. La capacità dell'Europa di esercitare il potere normativo in materia di sicurezza si scontra, come detto, con un forte impedimento legale: secondo l'Articolo 4(2) del Trattato sull'Unione Europea: "*L'Unione rispetta le funzioni essenziali dello Stato, inclusa [...] la salvaguardia della sicurezza nazionale. In*

[61] F. BALESTRIERI, L. BALESTRIERI, *Guerra digitale Il 5G e lo scontro tra Stati Uniti e Cina per il dominio tecnologico,* LUISS University Press, Roma 2019, M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance,* cit.

[62] si veda F. BALESTRIERI, L. BALESTRIERI, *op. cit.*

particolare, la sicurezza nazionale resta di esclusiva responsabilità di ciascuno Stato membro".

5. Il GDPR e le "ragioni di sicurezza nazionale"

Attraverso una tattica di governance che fa perno sulla "categoria del rischio[63]" quale principale "*proxy* trasduttiva"[64] tra

[63] 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 Data Protection & Privacy Law, 2020. Per l'analisi della differenza tra *risk approach* e *risk-based approach* si vedano: G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches, Connecting Constitutional Dots in the Digital Age*, in «Common Market Law Review» 2022, pp.473-500: gli autori chiariscano che 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 f*rame* come strumento per dare priorità e indirizzare l'azione di contrasto in modo proporzionato al pericolo effettivo: in altre parole, tende a "calibrare" l'applicazione della legge sulla base di punteggi di rischio concreti.

[64] In generale, un *proxy* è un sostituto o un rappresentante di qualcos'altro. Nel contesto del machine learning, spesso si riferisce a una variabile o a un modello utilizzato per approssimare o rappresentare un altro concetto o entità più complessa, ed è esattamente questo il ruolo che, fuor di metafora, la categoria del rischio come tecnica di normazione sembra assumere. Tale categoria è infatti utilizzata a partire dal GDPR (e con declinazioni parzialmente diverse con il DSA l'AI-Act) come principale tecnica di governance adottata dalla UE per promuovere i diritti fondamentali e i valori democratici quali "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 per il Mercato Unico Digitale, l'obiettivo non sarebbe quello di minimizzare i rischi a tutti i costi imponendo precauzioni massime (c.d. costituzionalismo precauzionale), ma raggiungere quella che è definibile come un' ottimizzazione del rischio (*consitutional optimization*). Sul tema, si rimanda ancora a G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches, Connecting*

"costituzionalismo sociale[65]" e "costituzionalismo politico" il GDPR (Reg. UE 2016/67911) si è rivelato strategicamente efficace imponendosi come *benchmark* a livello mondiale nella tutela dei diritti. Tuttavia, ha scontato, e sconta, l'assenza di una politica euro-unitaria in materia di trasferimento e monetizzazione dei dati[66]. La mancata elaborazione di una prospettiva strategica comune rischia 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[67].

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 dipenderà dai modi in cui il diritto positivo e la giurisprudenza definiscono la regolazione della sicurezza in ambito nazionale, trovando, così, geometria ed estensione variabile a seconda dell'effettivo bilanciamento tra questa e la tutela dei diritti fondamentali nei rispettivi ordinamenti. Su questa base, il considerando 16 permettendo, ai singoli Stati Membri di non attuare la normativa quando ad essere in ballo sono la sicurezza nazionale e/o l'interesse geopolitico, ben potrebbe legittimare l'eventuale

---

Constitutional Dots in the Digital Age, p. 21. Allo stesso tempo, la definizione normativa dei livelli di rischio accettabile, è lo strumento di traduzione normativa di tali contro-limiti, dotando così di efficacia i principi elaborati nel framework di un costituzionalismo «spontaneo», quale appunto è il costituzionalismo digitale (cfr. nota *supra*), tramite il recupero dalla centralità del momento politico (*Political costitutionalism*) e, segnatamente, della deliberazione democratica nell'amministrazione dei diritti fondamentali. Cfr. A. VERMEULE, *The Constitution of Risk*, Cambridge 2014.

[65] Cfr. *supra* nota 4.

[66] 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).

[67] Su questo punto si veda in particolare 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», IV, n. 1, 2022.

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[68].

Ciò significa che gli standard di tutela così come pensati dalla UE nel *framework* del costituzionalismo digitale, dovranno confrontarsi, da un lato, con possibili differenti obiettivi strategici in ambito regionale, dall'altro e soprattutto, con i differenti impianti costituzionali delle democrazie d'oltreoceano, dove il rapporto tra sicurezza nazionale - in particolare le esigenze governative di accesso e raccolta dati e tutela dei diritti individuali -è 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 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 – decidanodi integrare i dati che vengono raccolti nel loro territorio con l'amministrazione americana, sostanzialmente bypassando la normativa GDPR[69]. Dal canto loro,

---

[68] sulle ragioni che giustificano la necessità di rafforzare la sovranità tecnologica europea a scapito di quella degli Stati membri M. E. BARTOLONI, *op.cit.*

[69] Cfr. E. SCHMIDT, *op. cit.*, 2020a, pp. 25-27. La vicenda che coinvolto Tik Tok si inserisce nel crescendo di tensione che ha visto ad esempio un nuovo "*Clean Network programme*" che mira a tenere fuori le aziende c.d. "*unsafe"* dalle infrastrutture statunitensi di cavi, cloud e app, la restrizioni all'esportazione come quelle imposte nel 2020 alla *Semiconductor Manufacturing International Corporation*, il più grande produttore cinese di semiconduttori, sulla base del fatto che i suoi prodotti presentano un "rischio inaccettabile" di essere appunto deviati per "uso militare" o ancora "sanzioni senza precedenti" contro il gruppo tecnologico cinese Huawei. Si veda in merito L. CERULUS, *Huawei sanctions underscore Europe's tech dependency*, in "Politico", August 25, 2020. Marietje Schaake, sottolineando come l'amministrazione Trump abbia fatto all'epoca attivamente pressioni sui Paesi europei e su altri Paesi affinchè seguissero l'esempio di Washington vietando Huawei, parla a proposito di un

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[70], l'innovazione tecnologica americana subirebbe un evidente rallentamento lasciando il primato indiscusso alla Cina[71]. Emblematica rappresentazione della divergenza di obiettivi tra capitalismo politico americano[72] nel mercato dei dati e approccio europeo è il rapporto finale della Commissione nazionale di sicurezza 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» (National Security Commission On Artificial Intelligence, Final Report, 2021, p. 263.)

"Washington Effect" che potrebbe sostituire il "Brussels Effect". Cfr. M. SCHAAKE, *EU risks being dethroned as world's lead digital regulator*, in "Financial Times", August 23, 2020. Si veda anche *id. The Tech Coup: How to Save Democracy from Silicon Valley,* Princeton University Press, 2024, pp. 37 e ss.

[70] il GDPR pur non andando ad incidere sulla capacità di innovazione tecnologica per le aziende, rappresenta sicuramente un limite all'interferenza governativa nella raccolta dati a scopi strategici, come reso di plastica evidenza dal terremoto giudiziario seguito all'invalidazione del *Piracy Shield (*e quindi la possibilità di trasferire dati oltre oceano) da parte della CGUE con la "sentenza costituzionale" emessa nel caso *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Caso C-311/18, "Schrems II"). In merito si veda T. Christakis, *op. cit.*

[71] Su questo rischio si veda E. SCHMIDT, *I Used To Run Google. Silicon Valley could Lose to China*, in "The New York Times", 27 February, 2020. Sulla crescente similitudine di strategie tra Stati Uniti e Cina: M. LEONARD, A. DWORKIN, *Can Europe save the world order?* In «European Council of Foreign Relations (ECFR)» 260, 2018.

[72] Su obiettivi e sfide del nuovo capitalismo politico americano si veda A. ARESU, *op.cit.*

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 e ciò 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 la responsabilità, la trasparenza o la protezione dei diritti individuali.

Anche gli strumenti giuridici a disposizione (quali il *Committee on Foreign Investments in the US* (CFIUS)[73] e l'*International Emergency Economic Powers Act (*IEEPA) vengono utilizzati in tal senso e giustificati dalla retorica securitaria. Se i dati sono da considerarsi a tutti gli effetti come un asset decisivo per la sicurezza nazionale data la loro rilevanza in campo bellico, le aziende straniere che li raccolgono saranno considerate *infrastrutture critiche* e per operare negli USA – dovranno passare necessariamente per un'istruttoria del CFIUS che può concludersi con *executive order* del Presidente - non sindacabile a livello giurisdizionale- o ancora, legittimano il ricorso agli strumenti previsti dallo IEEPA utilizzabile appunto "*per affrontare una particolare e straordinaria minaccia [...] alla sicurezza nazionale, alla politica estera, o all'economia degli Stati Uniti*[74]*"*.

---

[73] Sui concetti di infrastruttura critica e di sicurezza nazionale, concetti questi, che si evolvono ridefinendosi continuamente, sulla base delle nuove tecnologie e dei nuovi obiettivi geostrategici che le potenze cercano di perseguire e che non è possibile definire a priori: «*la sicurezza nazionale, per un impero, è ciò che esso vuole che sia per mantenersi»* A. ARESU, *op.cit.* 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, p. 1.

[74] *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?

Paradigmatica è la vicenda che ha coinvolto TikTok[75] in cui gli USA hanno consapevolmente deciso di utilizzare lo IEEPA in funzione anti-cinese, con la decisione di "*bannare*[76]*"* 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. Lo strumento poteva quindi essere utilizzato come deterrente, per imporre 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[77]. Lo IEEPA è stato al contrario utilizzato come arma geo-economica nel tentativo di forzare la vendita di TikTok ad un'azienda statunitense[78] con l'obiettivo di continuare ad estrarre dati, tramite il più avanzato algoritmo della piattaforma cinese, ma assicurandone la proprietà americana. La tutela dei diritti individuali non è un problema che sembra sia entrato a far parte del ragionamento.

6. 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

---

[75] 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. Si veda anche D. MCCABE, *What's Going On With TikTok?, Here's What We Know*, New York Times, 1-2020, www.nytimes.com/2020/08/01/

[76] Ossia di bloccarla ed oscurarla sul proprio territorio.

[77] Così G. DE RUVO, *op. cit.* secondo cui lo scopo primario sarebbe stato "garantire che i dati vadano ad implementare l'IA a stelle strisce e non quella cinese".

[78] Si veda H. KISSINGER, E. SCHMIDT, D. HUTTENLOCHER, *The Age of AI and Our Human Future*, John Murray Publishers, 2021.

sicurezza nazionale, quale presupposto ideologico della normalizzazione della sorveglianza.

Negli USA la prevalenza delle esigenze governative di raccolta dati per lo sviluppo dell'IA sui diritti individuali è legittimata da quell'atmosfera "dataista"[79]che vede la sicurezza nazionale come esigenza a priori 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, come detto, a strumentalizzazioni politiche volte a giustificare limitazioni anche estreme della libertà personale.

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 in senso ampio come diritto all'identità individuale) deve fondarsi su una base giuridica adeguatamente accessibile (trasparente) prevedibile e formulata con sufficiente chiarezza da poter essere compresa, e dato gli attuali limiti posti dalla sovranità statale, il modo in cui il diritto positivo e la giurisprudenza degli Stati Membri vi accorderanno tutela nel bilanciamento con le ragioni dei sicurezza, non solo incide sulla complessiva struttura del sistema politico e giuridico del Paese, ma determina in concreto anche la compatibilità di quei sistemi con il fulcro dell' identità internazionale (e costituzionale) europea.

Il framework del "costituzionalismo digitale" che di tale identità è espressione, è infatti non solo fattore di legittimazione della sovranità digitale 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 "governance algoritmica" pubblica e/o privata che, sebbene strumento

[79] Sul concetto di "dataismo" coniato da Van Dijk cfr. *supra* nota 38.

d'innovazione tecnologica, non sia lesiva dei diritti fondamentali del singolo, sono due gli aspetti che si è cercato di mettere in rilievo nel corso di questa analisi. La necessità da un lato, di "de-naturalizzare" i presupposti ontologici del modello aziendale alla base del capitalismo computazionale, che legittima e normalizza i descritti processi di datificazione o "espropriazione identitaria". Dall'altro l'opportunità di interrogarsi sulle possibilità effettivamente offerte dall'attuale architettura costituzionale dell'Unione all'acquisizione e alla costruzione di quell' autonomia strategica che la sovranità digitale, intesa come capacità di tutela normativa della propria identità valoriale, necessariamente presuppone. Il c.d. approccio integrato delle competenze in materia di sicurezza[80] 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, una visione integrata delle varie politiche si porrebbe inevitabilmente in contrasto con il principio d'attribuzione 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

[80] 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 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, p. 13. https://data.consilium.europa. eu/doc/document/ST-7371-2022-INIT/it/pdf

unitaria[81]. Come si è cercato di porre in evidenza, riconoscere all'UE le prerogative necessarie perché si possa parlare di sovranità digitale europea è, allora, precondizione alla realizzazione di un costituzionalismo digitale che possa dirsi di natura non soltanto "procedurale", ma anche "sostanziale".

[81] Sul tema si veda ampiamente M.E. BARTOLONI, *op.cit.*, 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, con dicitura non priva di suggestione, qualifica come «mercato europeo della difesa»; Cfr. Comunicazione della Commissione COM (2022) 60 final, *cit.*