IPE BUSINESS SCHOOL

DIRITTO E TECNOLOGIA

European Digital Strategy: il *favor* per l'attore pubblico

di Giovanni Orlacchio

IPE Working Paper

N. 24

August 2, 2024

DIRITTO E TECNOLOGIA

European Digital Strategy: il *favor* per l'attore pubblico

di Giovanni Orlacchio*

Abstract

Come è disciplinato l'utilizzo dei dati personali da parte dell'attore pubblico? Questo *paper* approfondisce l'impostazione della *European Digital Strategy*, evidenziando le norme di diritto positivo e gli obiettivi del Legislatore eurounitario. Partendo dal GDPR, lo scritto puntualizza la continuità di un certo *favor*, sia nel *Data Act* che nell'*Artificial Intelligence Act*. In particolare, sono analizzati i parametri d'eccezione utilizzati dal regolatore, dall'«emergenza pubblica» al «compito specifico di interesse pubblico». Lo scritto si sofferma anche su una particolare novità: l'obbligo di messa a disposizione dei dati detenuti dai privati ex art. 14 Data Act su richiesta dell'attore istituzionale. Durante l'analisi dell'AI Act è stata rimarcata la pluralità di *telos* perseguibili nello sviluppo di *AI System* all'interno di appositi spazi di sperimentazione normativa. Infine, in sede di conclusioni, rimarcata la cornice minima delle garanzie, si propone la necessità di fare un ulteriore passo: occuparsi del tema direttamente invece che per vie "implicite".

Parole o frasi chiave: *European Digital Strategy – GDPR – Data Act – AI Act – e-Democracy*

* Dottore in Giurisprudenza, laureatosi con lode presso l'Università degli Studi di Napoli Federico II il 17/07/2024, con una tesi in Diritto Costituzionale dal titolo *Intelligenza artificiale e dati dei cittadini nelle politiche pubbliche*, sotto la guida della Chiarissima Prof.ssa Giovanna De Minico.
Email: giovanni.orlacchio@outlook.com – LinkedIn: www.linkedin.com/in/giovanni-orlacchio-412aa9129.

Indice

1. La strategia digitale dell'Unione Europea

Tra gli obiettivi del mandato 2019-2024 la Presidente della Commissione Ursula von der Leyen ha posto al punto 3 il *goal*: «Un'Europa pronta per l'era digitale»[1]. Trovandoci alla fine di questo quinquennio – e attendendo con curiosità i numerosi atti attuativi, a partire dall'implementazione di *standard* adeguati[2] – possiamo affermare la parziale conformità tra propositi e passi in avanti compiuti. Il contributo politico e normativo[3] della strategia digitale europea[4] – composta principalmente da: *General Data Protection Regulation* (GDPR)[5] e Reg.

[1] U. VON DER LEYEN, *Un'Unione più ambiziosa – Il mio programma per l'Europa, orientamenti politici per la prossima Commissione europea 2019-2024*, 16 luglio 2019, pp. 14-15.

[2] In particolare circa il *Fundamental Rights Impact Assessment* (FRIA) ex art. 27 AI Act: C. NOVELLI, *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in *federalismi.it*, n. 2/2024, 95-113, p. 110 e ss.; I. YORDANKA, *The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI*, disponibile in SSRN, in *Springer Proceedings of the Annual Privacy Forum* (Lisbon, 2020), 20. Si veda per una panoramica sugli *standard*: H. POUGET e R. ZUHDI, *AI and Product Safety Standards Under the EU AI Act*, in *CarnegieEndowment.org*, il 5.03.2024: «The EU's AI Act marks a critical step toward regulating the fast-evolving field of artificial intelligence, setting a precedent for global digital regulation. However, its success hinges on the effective translation of its high-level safety requirements into precise, actionable standards by CEN and CENELEC. Comparisons with standards providing guidance for risk assessment and mitigation in established safety-critical sectors reveal the need for standards that are not only detailed and legally certain but also flexible enough to accommodate the unique characteristics of AI technologies». Per una analisi più specifica: J. LAUX, S. WACHTER and B. MITTELSTADT, *Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act*, in *Computer Law & Security Review*, n. 53/2024, 11; J. LAUX, S. WACHTER and B. MITTELSTADT, *Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and the Acceptability of Risk*, in *Regulation & Governance*, 02/2023, 34.

[3] Sul tema si veda: A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'Intelligenza Artificiale*, in *Studi parlamentari e di politica costituzionale*, n. 1/2021, 31-52, p. 51: «la strada imboccata dall'Europa con questa poderosa operazione di recupero della centralità delle fonti del diritto è quella giusta, perché può consentire di affrontare correttamente il tema della sovranità e del potere nell'era digitale, che rappresenta uno dei problemi più rilevanti del costituzionalismo del XXI secolo».

[4] Per una visione chiara e completa della strategia digitale europea si veda sul sito della Commissione: Un'Europa pronta per l'era digitale; particolarmente utile può risultare la cronologia degli atti presente in basso alla pagina web. Per una analisi complessiva: Y. POULLET, *Towards a New EU Regulatory Approach of the Digital Society*, in *European Review of Digital Administration & Law – ERDAL*, Volume 3, Issue 1, 2022, 113-124.

(UE) 2018/1725[6] quali prime vere normazioni sulla materia; *Data Governance Act* (DGA)[7], *Digital Market Act* (DMA)[8], *Data Act* (DA)[9], *Interoperable Europe Act* (IEA)[10] trasversalmente sui dati; e *Digital Services Act* (DSA)[11], *Cyber Security Act* (CSA)[12], *Artificial Intelligence Act* (AI

---

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati – GDPR).

[6] Il Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati.

[7] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati – DGA). Si vedano anche: A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'Intelligenza Artificiale*, cit., a p. 31 sugli obiettivi del DGA; N. MACCABIANI, *The European path towards data quality and its standardisation in AI: a legal perspective*, in *BioLaw Journal – Rivista di BioDiritto*, n. 4/2022, 473-502, in particolare p. 483 e ss.; S. TORREGIANI, *La disciplina europea dei dati: dalla protezione alla governance*, Tesi di dottorato 2022, Università degli studi di Macerata, 317, p. 214 e ss. sulle finalità di DGA e DA, in particolare p. 218 e ss. circa la struttura di *governance open, fair* e *democratic*, i pro e i contro del *data sharing*.

[8] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali – DMA). Si veda: G. DE MINICO, *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e neurodiritti*, in *federalismi.it*, n. 6/2024, 21, p. 14 e ss.

[9] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati – DA). Il DA è entrato in vigore il 14 gennaio 2024 e sarà applicabile dal 2025.

[10] Regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio del 13 marzo 2024 che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile – IEA).

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

[12] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (regolamento sulla cibersicurezza – CSA).

Act)[13] su questioni più specifiche; oltre che dall'istituzione di varie *Authority*, *in primis* l'AI Office[14] – sta creando le condizioni infrastrutturali per favorire un'innovazione sostenibile nel

[13] La procedura europea è iniziata con la Proposta di Regolamento del Parlamento Europeo e del Consiglio, che ha stabilito regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) 2021/0106(COD), 21/4/21, in https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206. A essa sono seguiti l'Orientamento generale del Consiglio dell'Unione Europea, 6/12/22 e poi gli emendamenti del Parlamento Europeo, 14/6/23. Quindi, il Trilogo ha chiuso l'accordo su un testo comune il 9/12/23, approvato poi dal Comitato dei Rappresentanti Permanenti il 2/2/2024 e definitivamente dal Parlamento europeo il 13/3/2024. Il testo è stato pubblicato in gazzetta ufficiale dell'UE il 12/07/2024: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=OJ%3AL_202401689. Per i lavori dell'arco temporale 2021-2024 si veda il sito ufficiale https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A52021PC0206.

[14] Previsto dall'art. 65 AI Act, con la decisione C/2024/1459 della Commissione europea del 24.01.2024 viene l'Ufficio europeo per l'intelligenza artificiale "AI Office". A motivazione della decisione, i *considerandа* 4 e 5 prevedono: «È necessario sviluppare competenze e capacità a livello dell'Unione al fine di accrescere tale comprensione, di contribuire all'attuazione e all'applicazione del regolamento di prossima adozione che stabilisce regole armonizzate sull'intelligenza artificiale e di contribuire all'attuazione delle norme e dei principi internazionali in materia di IA, quali il codice di condotta e i principi guida approvati dal G7 per gli sviluppatori di sistemi di IA avanzati»; «In tale contesto è opportuno gettare le basi per un sistema di governance unico per l'IA nell'Unione, attraverso l'istituzione di una struttura che dovrebbe essere incaricata della vigilanza dei progressi compiuti nel campo dei modelli di intelligenza artificiale, anche per quanto riguarda i modelli di IA per finalità generali, e dell'interazione con la comunità scientifica, e che dovrebbe svolgere un ruolo fondamentale nelle indagini, nei test e nell'applicazione delle norme, e avere una vocazione globale». L'AI Office ex art. 1 par. 2 della decisione C/2024/1459 della Commissione fa parte della struttura amministrativa della direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie. Il Connect – Communications Networks, Content & Technology è attualmente diretto dall'italiano Roberto Viola e presenta un organigramma molto cospicuo; è sottoposto alla direzione politica del Commissario per il Mercato Interno. Da notare il *considerandum* 6 alla decisione 2024/1459 della Commissione: «L'Ufficio europeo per l'intelligenza artificiale dovrebbe operare conformemente ai processi interni della Commissione (6) e la sua istituzione non dovrebbe pregiudicare i poteri e le competenze delle autorità nazionali competenti né degli organi e degli organismi dell'Unione per quanto riguarda la vigilanza dei sistemi di IA, come previsto dal regolamento di prossima adozione che stabilisce regole armonizzate sull'intelligenza artificiale e da altre legislazioni settoriali dell'Unione. Esso lascia impregiudicate le funzioni di altri servizi della Commissione nei rispettivi settori di competenza, nonché quelle del servizio europeo per l'azione esterna nel settore della politica estera e di sicurezza comune. L'Ufficio europeo per l'intelligenza artificiale dovrebbe svolgere i propri compiti, in particolare quello di fornire orientamenti, in modo tale da non duplicare le attività dei pertinenti organi e organismi dell'Unione a norma della legislazione settoriale», la nota 6 recita: «Non si tratta di un ufficio europeo ai sensi dell'articolo 2, punto 26), del regolamento finanziario (regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18

mercato unico dell'UE. Con il governo dell'innovazione per il tramite del diritto[15] inizia a prendere forma il contesto normativo per la costruzione dello *european digital market*[16].

Le finalità politiche comuni[17] – quali conquistare la «sovranità digitale»[18], perseguire obiettivi industriali[19] e influenzare il diritto globale con il c.d. *Brussels effect*[20]– sono sempre più chiare e tangibili.

---

luglio 2018)», punto 26 che prevede la definizione di «ufficio europeo»: «una struttura amministrativa creata dalla Commissione, o dalla Commissione insieme a una o più altre istituzioni dell'Unione, per svolgere funzioni orizzontali specifiche». Si veda anche: K. ZENNER, P. HACKER and S. HALLENSLEBEN, *A vision for the AI Office: Rethinking digital governance in the EU*, in *Euractive*, il 23 maggio 2024.

[15] G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del Diritto*, n. 2/2019, 199-236, p. 233: «Non ci si dovrebbe ispirare a un *laissez-faire* tecnologico, né a un luddismo di retroguardia. È invece necessario operare, in tutte le sedi, perché i processi in atto, i quali sono destinati a regolare segmenti crescenti della vita sociale dell'uomo, siano sottoposti a una logica di controllo democratico, che assicuri un adeguato bilanciamento tra la «funzionalità tecnologica» e la desiderabilità sociale degli scopi perseguiti, e rispetto alla quale la mediazione giuridica svolge un ruolo centrale». Si veda anche T. CASADEI, *Il senso del 'limite' - Montesquieu nella riflessione di Hannah Arendt*, in D. FELICE (*a cura di*), *Montesquieu e i suoi interpreti*, Pisa, Ets, 2005, tomo II, 805-838, in particolare pp. 817-818: «la permanenza delle leggi è il caposaldo fisso cui ancorare l'innovazione. Le leggi si connotano – questo l'esito del ragionamento arendtiano che parte dalla scoperta di Montesquieu per giungere ad un originale approdo – nella duplice forma di confini, intendendo questo concetto sia come limite sia come relazione. I confini si configurano come la fonte originaria dello spazio pubblico-politico, in cui si danno regole e possibilità di comunicazione. Nella prospettiva arendtiana, qualsiasi cosa (dunque, anche le istituzioni) prende forma attraverso i limiti, donde la forza insita nell'idea stessa del limite, forza non solo 'limitante', ma generatrice di possibilità (dunque 'abilitante')».

[16] S. TORREGIANI, *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in *Rivista italiana di informatica e diritto*, 2021, 47-65, pp. 48-49: «la creazione del "Mercato Unico Digitale", concepito nelle intenzioni delle istituzioni europee come un passo imprescindibile affinché il mercato interno possa continuare a funzionare nell'era della digitalizzazione. Oggi è, difatti, impossibile condurre un'attività economica con caratteri transfrontalieri senza far fronte a tutte le questioni connesse al tema del trasferimento delle informazioni: i dati devono necessariamente muoversi assieme al bene al quale ineriscono, pertanto, in un mercato in cui gli ostacoli allo spostamento di persone, merci, capitali e servizi sono stati abbattuti, è chiaro che l'incentivo alla libera circolazione delle informazioni si manifesta come un passaggio irrinunciabile». Circa i risvolti economici, tra gli altri: M. BORGHESE, *Mercato unico digitale: la strategia europea dei dati e le 2 velocità*, in *ilSole24Ore*, il 22.12.2023: «Per rimuovere le principali limitazioni e far acquisire all'UE una posizione di leadership in una società basata sui dati, la nuova strategia punta ad un sistema di regolamentazione che incentivi la creazione e la circolazione dei dati, agevolando la valorizzazione del relativo potenziale informativo».

[17] In quanto solo in una dimensione europea raggiungibili. Si veda, *ex multis*: *considerandum* 170 General Data Protection Regulation: «Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo»; *considerandum* 63 *Data Governance Act*: «Poiché gli obiettivi del presente regolamento, ossia il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici, nonché l'istituzione di un quadro di notifica e controllo per la fornitura di servizi di intermediazione dei dati e di un quadro per la registrazione volontaria delle entità che mettono i dati a disposizione a fini altruistici e di un quadro per l'istituzione di un comitato europeo per l'innovazione in materia di dati, non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della loro portata e dei loro effetti, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo».

[18] *Ex multis*: A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'Intelligenza Artificiale*, cit., p. 34: «L'Ue intende procedere, quindi, nella direzione indicata dalla Presidente della Commissione europea, Ursula von der Leyen, già al suo insediamento, vale a dire il perseguimento dell'indipendenza digitale europea da America e Cina e il bilanciamento tra la governance dello sviluppo tecnologico e le esigenze sociali, nel nome dell'affermazione della sovranità digitale europea»; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, 63-89, in particolare p. 67 e ss. sul rapporto tra sovranità e potere cibernetico.

[19] S. TORREGIANI, *La disciplina europea dei dati: dalla protezione alla governance*, cit., pp. 5 e 12 circa i ritardi europei rispetto ai *competitor* USA e Cina e all'utilizzo del diritto per riguadagnare terreno ed evitare fuoriuscite preziose di dati. Si veda anche la relazione alla proposta di regolamento COM/2022/68 (*Data Act*), p. 7: «In linea con la strategia industriale la proposta riguarda tecnologie altamente strategiche quali il cloud *computing* e i sistemi di intelligenza artificiale, settori il cui pieno potenziale non è ancora stato sfruttato dall'UE, all'alba della prossima ondata di dati industriali. Essa attua l'obiettivo della strategia per i dati di far sì che le imprese siano maggiormente in grado di innovare e di essere competitive sulla base dei valori dell'UE, e il principio della libera circolazione dei dati nel mercato interno. La proposta è inoltre coerente con il piano d'azione sulla proprietà intellettuale in cui la Commissione si è impegnata a riesaminare la direttiva sulle banche di dati. La presente proposta dovrebbe inoltre rispettare i principi del piano d'azione sul pilastro europeo dei diritti sociali e i requisiti di accessibilità della direttiva (UE) 2019/882 sui requisiti di accessibilità dei prodotti e dei servizi».

[20] A. BRADFORD, *The Brussels Effect – How the European Union Rules the World*, New York, Oxford University Press, 2020, 404, p. 1 e ss.: «The term the "Brussels Effect" refers to the EU's unilateral ability to regulate the global marketplace. The Brussels Effect can be unintentional, arising from a set of enabling conditions sustained

L'Unione, consapevole dei ritardi nel mercato delle tecnologie più di frontiera[21], ha deciso di "giocare in attacco" utilizzando i suoi *asset* principali: mercato interno e avanguardia normativa. L'intera strategia digitale europea scommette sulla

> «ability to promulgate regulations that shape the global business environment, leading to a notable "Europeanization" of many important aspects of global commerce. Different from many other forms of global influence, the EU does not need to impose its standards coercively on anyone—market forces alone are often sufficient to convert the EU standard into the global standard as companies voluntarily extend the EU rule to govern their worldwide operations. Under specific conditions, the Brussels Effect leads to "unilateral

---

by markets rather than from the EU's active efforts to export its regulations. While acknowledging that other forms of the EU's global influence exist, this book generally reserves the term the Brussels Effect to capture the phenomenon where the markets are transmitting the EU's regulations to both market participants and regulators outside the EU. In these instances, the EU does not have to do anything except regulate its own market to exercise global regulatory power. The size and attractiveness of its market does the rest. Thus, in essence, the Brussels Effect emerges from market forces and multi- national companies' self-interest to adopt relatively stringent EU standards globally. At the same time, the Brussels Effect is not only the result of private power: it is the interplay between EU regulations and the market forces' ability to externalize those regulations in different markets that give rise to the Brussels Effect. Further, there are two variants of the Brussels Effect: the "de facto Brussels Effect" and the "de jure Brussels Effect." The de facto Brussels Effect explains how global corporations respond to EU regulations by adjusting their global conduct to EU rules. No regulatory response by foreign governments is needed; corporations have the business incentive to extend the EU regulation to govern their worldwide production or operations. The de jure Brussels Effect—which refers to the adoption of EU-style regulations by foreign governments—builds directly on the de facto Brussels Effect: after multinational companies have adjusted their global conduct to conform to EU rules, they have the incentive to lobby EU-style regulations in their home jurisdictions. This ensures that they are not at a disadvantage when competing domestically against companies that do not export to the EU and that, therefore, have no incentive to conform their conduct or production to costly EU regulations».

[21] «Il mercato dell'IA è attualmente dominato dalle due maggiori economie globali, USA e Cina, che si stanno giocando il primato di Paese più avanzato del globo a colpi di investimenti in innovazione. Nel confronto globale, gli Stati Uniti coprono il 36% dei ricavi complessivi, seguiti da Cina (12%), Germania (4%) e Regno Unito (4%). L'Italia non va oltre il 2%, posizionandosi comunque all'ottavo posto a pari merito con l'Australia […] Focalizzando l'attenzione sull'UE, la Francia, la Germania e la Svezia si collocano sul podio con un volume di investimenti venture capital che complessivamente copre circa il 65% degli investimenti VC totali in UE. L'Italia si classifica ancora una volta solo in ottava posizione (204 milioni di dollari) dietro anche ad economie più piccole come Romania, Spagna e Irlanda» in M.R. DELLA PORTA e D. SALERNO, *RAPPORTO I-COM IA, gravi ritardi per Europa e Italia: lo dicono i dati*, in *Agenda Digitale*, il 6.11.2023.

regulatory globalization," where regulations originating from a single jurisdiction penetrate many aspects of economic life across the global marketplace»[22].

Il potere normativo dell'UE punta a produrre effetti non solo per i nostri cittadini, consumatori e imprese, ma per l'intero *global market*, anche dell'*artificial intelligence*[23]. Considerando il ruolo assunto dal GDPR[24], col quale «The EU sets the tone globally for privacy and data protection regulation»[25], non ci sono molte voci discordanti[26] sulla possibilità che

---

[22] A. BRADFORD, *The Brussels Effect – How the European Union Rules the World*, cit., p. XIV.

[23] Per approcciarsi al tema, molto *user friendly* risulta essere questo *smart panel* prodotto dal World Economic Forum: https://intelligence.weforum.org/topics/a1Gb0000000pTDREA2 . Non è semplice stare al passo dei vari *trend* e sviluppi legati all'intelligenza artificiale, una guida affidabile può trovarsi negli aggiornati Insights on Artificial Intelligence sul sito di McKinsey. Circa l'utilizzo dell'identificativo "intelligenza artificiale" per indicare queste tecnologie: «Rispettata la sua natura di *umbrella concept*, ha il nocciolo identitario nei processi di apprendimento, guidati dalla mente umana ma capaci di evoluzione autonoma – nutriti da masse crescenti di dati – che con valutazioni automatiche si risolvono nel contenuto di decisioni pubbliche o private. […] Il modo di procedere dell'I.A passa attraverso due snodi importanti. Il primo riguarda il suo metodo di ragionamento: di tipo statistico-correlazionale, che impiega per anticipare con valutazione prospettica l'accadimento di certe situazioni secondo l'*id quod plerumque accidit*. Il secondo snodo riguarda invece gli effetti dell'agire intelligente, tendenti a conformare o almeno orientare la condotta di collettività di soggetti» in G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Rivista AIC*, n. 2/2024, 85-108, p. 86.

Circa l'impatto economico, si veda questo *report* di PWC: *Sizing the prize PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution What's the real value of AI for your business and how can you capitalise?*. Forse molti lavori verranno sostituiti dalle macchine, ma altrettanti se non di più verranno creati dalle nuove tecnologie. Sul punto si veda: H. EKELUND, *Why there will be plenty of jobs in the future — even with artificial intelligence*, pubblicato il 26.02.2024 sul sito del World Economic Forum. Circa i possibili effetti per le pubbliche amministrazioni, si veda: G. DOMINICI, *Intelligenza artificiale nella Pa: come gestire al meglio una trasformazione epocale partendo dalle persone*, in *ilSole24Ore*, il 22.03.2024. Non sono da dimenticare poi i rischi per la democrazia, e.g. circa la disinformazione all'interno di un mercato libero delle idee. Ad esempio, tramite i c.d. *deep fake* che ex art. 3 punto 60 AI Act sono: «un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi o altre entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona». Si veda, *ex multis*: C. PINELLI, *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in *Diritto Pubblico*, n. 1/2022, 173-197.

[24] A. BRADFORD, *The Brussels Effect – How the European Union Rules the World*, cit., p. 131 e ss.

[25] Ivi, p. 132.

[26] Si veda: M. ALMADA and A. RADU, *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, in *German Law Journal*, 2024, 1–18.

accada lo stesso. In particolare, circa l'*Artificial Intelligence Act,* forse proprio la scelta regolatoria di impostare il controllo *ex ante* nelle mani degli stessi privati[27] – obbligati ad autovalutarsi secondo gli *standard* della categoria di rischio[28] di riferimento[29] – oltre a rispondere ad esigenze pratiche potrà essere la chiave di successo interna e di diffusione extraeuropea dell'AI Act. Secondo chi scrive, infatti, questa modalità elastica e di fiducia nell'operatore privato si spiega anche con la necessità di *non-divisibility* delle multinazionali *tech*[30], le quali in tal modo saranno meglio predisposte ad adattarsi – anche globalmente – agli

[27] G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, cit., p. 87: «Il controllo anticipato, apprezzabile come idea, è invece deludente nella realizzazione in quanto il legislatore non ha obbligato il fornitore a sottoporre la macchina a un certificatore esterno e pubblico, accontentandosi di una sua semplice autodichiarazione, c.d. *self-compliance*, che attesti il rispetto della disciplina prudenziale. La coincidenza soggettiva tra controllato e controllante, cioè questo fisiologico conflitto di interessi, compromette l'obiettività del sindacato, strutturalmente inadatto a offrire quelle garanzie di neutralità necessarie a rassicurare i terzi. Eppure l'*A.I.Act* conosce il modello del controllo preventivo affidato al terzo, che impiega in situazioni residuali e tassative (art. 43, par. 1, co. 2) perché oneroso per il privato».

[28] L'AI Act prevede all'art. 3 punto 2 tale definizione di "rischio": «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso».

[29] Ricco di spunti e proposte: C. NOVELLI, F. CASOLARI, A. ROTOLO, M. TADDEO, L. FLORIDI, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, v. 3, article number 13, 2024. Ivi, pp. 2-3: «Accordingly, the risk of an event is assessed by the interplay between (1) determinants of risk (i.e., hazard, exposure, vulnerability, and responses), (2) individual drivers of determinants, and (3) other types of risk (i.e., extrinsic, and ancillary risks). This framework can provide a more accurate risk magnitude of AIs under a specific scenario. This is a measure defined based on hazard chains, the trade-of among impacted values, the aggregation of vulnerability profiles, and the contextualisation of AI risk with risks from other sectors. This qualitative analysis is grounded on a quantitative assessment. In fact, the risk magnitude should be assessed by weighing the fundamental values (positively and negatively) affected by AIs against the intensity of the interference of AIA's risk containment measures on the same values. This type of judgment for interference between constitutional principles is the object of the proportionality test by Robert Alexy (Alexy, 2002). The outcome of the test would indicate whether a risk category is appropriate for an AI under a specific risk scenario or whether it introduces grossly disproportionate limitations and trade-offs for competing values».

[30] A. BRADFORD, *The Brussels Effect – How the European Union Rules the World*, cit., p. 158: «the occurrence of the Brussels Effect in data privacy often comes down to the existence of non-divisibility. This chapter has shown how most multinational companies today maintain a global privacy policy that closely conforms to the GDPR, likely for reasons of both technical and economic non-divisibility as well as to minimize complexity and compliance errors. Non-divisibility is also driven by these companies' need to preserve a global brand and offer equal

obblighi imposti con il Regolamento. Focalizzandosi sul mercato e forse meno sui diritti dei singoli, il Legislatore ha preferito puntare ad un doveroso controllo *ex post* da parte delle Istituzioni europee e degli Stati membri; sebbene discutibile, dato l'alto tasso di tecnicità e la velocità con la quale l'innovazione tecnologica cambia le "carte da gioco", l'elasticità e la quasi assenza di un controllo *ex ante* non sono da giudicarsi come scelte completamente negative.

Quando il pacchetto di regolamenti attuativi della strategia digitale sarà completamente efficace, i cittadini e le imprese europee potranno contare su uno *european digital market* ricco di dati, in particolare industriali, pronti per essere utilizzati secondo un chiaro e avanzato assetto normativo[31]. La certezza del diritto è un elemento essenziale per fare innovazione e per la competitività del tessuto economico dei 27[32].

---

protections to all their users, in particular today when data protection issues have grown in salience and drawn global attention to the corporate practices in this regard».

[31] C. NOVELLI, F. CASOLARI, A. ROTOLO, M. TADDEO, L. FLORIDI, *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, cit., pp. 7-8: «The supranational legislator expects the regulation of AI to increase legal certainty in this feld and to promote a well-functioning internal market: reliable for consumers, attractive for investment, and technologically innovative. This might trigger the Brussels effect, ensuring a competitive advantage over other international policy-makers while shaping their regulatory standards (Bradford, 2020). Nevertheless, should the AIA prove to be unsustainable or ineffective, the EU may lose its attractiveness for the production and commercialisation of AI technologies. To prevent this, the AIA must introduce norms that promote safety while not disincentivising the production or deployment of AIs. In this regard, the AIA's risk-based approach has its strengths and weaknesses».

[32] Il Prof. Mario Draghi è stato «incaricato nei mesi scorsi dall'attuale presidente della Commissione Europea di misurare i livelli di competitività dell'Unione a 27. Draghi ha anticipato alcuni dati relativi al rapporto finale sulla competitività che sarà pronto a giugno, affermando con decisione che l'Europa dovrà investire somme ingenti per recuperare terreno e non rischiare di rimanere schiacciata tra i due giganti, USA e Cina, molto più avanzati del vecchio continente», in https://www.econopoly.ilsole24ore.com/2024/03/27/competitivita-draghi-aziende-italia/. Si legga M. DRAGHI, *Intervento alla High-Level Conference on the European Pillar of Social Rights*, a La Hulpe (Belgio), il 16 aprile 2024, pubblicato in italiano in *Rivista Eurojus*, n. 2/2024, 274-279. Si veda anche il rapporto sul mercato unico: E. LETTA, *Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, presentato il 18.04.2024. Sull'importanza di una normazione di qualità per sostenere l'innovazione e la competitività dell'UE si veda: https://www.uni.com/cen-e-cenelec-danno-il-benvenuto-alla-nuova-strategia-europea-di-normazione/.

Nell'era «datizzata»[33] è evidente che qualsiasi tentativo di regolare la tecnologia passa, necessariamente, per la gestione, la circolazione e l'utilizzo dei dati[34]. L'obiettivo di questo lavoro è evidenziare un certo *favor* che il Legislatore eurounitario ha verso l'utilizzo dei dati[35] da parte dell'attore pubblico.

---

[33] «Ciò che c'è di nuovo nell'epoca attuale sono il tasso di variazione della potenza di calcolo e la penetrazione delle tecnologie dell'informazione in ogni ambito dell'esistenza [...] Gordon Moore giunse alla conclusione che la tendenza da lui osservata sarebbe continuata a intervalli regolari, per cui le capacità dei processori dei computer sarebbero raddoppiate ogni due anni. La "legge di Moore" si è dimostrata sbalorditivamente profetica. La rivoluzione del calcolo ha introdotto per la prima volta tantissimi individui e processi nel medesimo mezzo di comunicazione e per la prima volta ha tradotto e tracciato le loro azioni in un unico linguaggio tecnologico [...] l'attività umana risulta sempre più "datizzata" e parte di un unico sistema "quantificabile e analizzabile"» in H. KISSINGER, *World Order*, trad.it. *Ordine mondiale*, Milano, Mondadori, 2015, 405, p. 339. I dati sono in costante aumento (https://explodingtopics.com/blog/data-generated-per-day) e nei prossimi anni con la diffusione di tecnologie *IoT (Internet of Things)* l'incremento sarà ancora maggiore: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ .

[34] S. CALZOLAIO, *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, n. 1/2021, 5-9, pp. 5-6 e pp. 7-8: «siamo in un contesto di *data-driven innovation*; l'innovazione si realizza attraverso lo sfruttamento dei dati. In tutti i settori, e trasversalmente. Ciò significa che anche la competizione e la concorrenza fra aziende, stati, continenti si gioca nella progressione della capacità di sfruttamento dei dati. Questi aspetti lasciano capire perché il possesso e la disponibilità dei dati sono strategici, per le imprese, per gli Stati, e per le imprese che operano nei diversi Stati. Di più. Questo momento storico caratterizzato dalla pandemia rende evidente che l'avvento della *datification* e la *data-driven innovation* conducono ormai ad un contesto di *data dependence*: non si tratta di sviluppare complessi ragionamenti, ma di arrendersi al fatto che il corso, il fluire, lo sviluppo della vita personale, sociale, economica, istituzionale dipende dal e segue il flusso dei dati. Siamo dipendenti dalla garanzia della continuità del flusso dei dati e delle informazioni per comunicare, esprimerci, operare, lavorare, vivere [...] Il diritto dei dati, pertanto, ha iniziato a porre limiti ed a porsi in contrapposizioni ai caratteri genetici della rete internet, che consentono l'ubiquità dei dati e potenzialmente lo sfruttamento dei dati in modo simultaneo e intensivo. Si sono affacciati nel contesto del dibattito scientifico i temi della localizzazione dei dati, della sovranità sui dati e della sovranità digitale dello Stato, il tema del regime del *trans-border data flow*, il rischio del *data colonialism*, o all'inverso del *digital isolationism*, e infine la nuova tendenza al *data nationalism*». Circa il *data nationalism*, si veda: A. CHANDER e P.L. UYÊN, *Data Nationalism*, in *Emory Law Journal*, vol. n. 64/2015, 677-740.

[35] Anche se questa sede non è adatta, è da tenere in mente che tale disciplina andrebbe studiata in combinato con la normativa inerente al processo decisionale algoritmico, seguendo la scia della prospettiva suggerita da: DATEN ETHIK KOMMISSION, *Opinion of the Data Ethics Commission – Executive Summary*, Berlino, Ottobre 2019,

2. Il GDPR e il Regolamento (UE) 2018/1725

Il Reg. (UE) 2016/679 (GDPR) è la vera architrave normativa del sistema, in particolare considerando il suo rapporto privilegiato con gli altri atti inerenti i dati[36] e l'intelligenza artificiale[37].

31, analizzata da S. TORREGIANI, *L'impatto dei dati non personali sulle decisioni algoritmiche: la prospettiva delle autorità amministrative indipendenti europee*, in *Osservatorio sulle fonti*, n. 2/2021, 807-829, p. 825 e ss.

[36] L'art. 1 par. 3 DGA prevede: «Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. In particolare, il presente regolamento non pregiudica i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680, anche per quando riguarda i poteri e le competenze delle autorità di controllo. In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o il diritto nazionale adottato conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680». Si veda anche il *considerandum* 7 al DA: «[...] Il presente regolamento integra e lascia impregiudicato il diritto dell'Unione in materia di protezione dei dati personali e della vita privata, in particolare i regolamenti (UE) 2016/679 e (UE) 2018/1725 e la direttiva 2002/58/CE. Nessuna disposizione del presente regolamento dovrebbe essere applicata o interpretata in modo da ridurre o limitare il diritto alla protezione dei dati personali o il diritto alla vita privata e alla riservatezza delle comunicazioni. Qualsiasi trattamento di dati personali a norma del presente regolamento dovrebbe rispettare il diritto dell'Unione in materia di protezione dei dati, tra cui il requisito di una valida base giuridica del trattamento a norma dell'articolo 6 del regolamento (UE) 2016/679 e, se del caso, e le condizioni di cui all'articolo 9 di tale regolamento e all'articolo 5, paragrafo 3, della direttiva 2002/58/CE. Il presente regolamento non costituisce una base giuridica per la raccolta o la generazione di dati personali da parte del titolare dei dati. Il presente regolamento impone ai titolari dei dati l'obbligo, dietro richiesta di un utente, di mettere i dati personali a disposizione degli utenti o di terzi scelti dall'utente. Tale accesso dovrebbe essere fornito ai dati personali trattati dal titolare dei dati sulla scorta di una delle basi giuridiche di cui all'articolo 6 del regolamento (UE) 2016/679. Se l'utente non è l'interessato, il presente regolamento non costituisce una base giuridica per consentire l'accesso ai dati personali o per mettere i dati personali a disposizione di terzi e non dovrebbe essere inteso nel senso che conferisce al titolare dei dati un nuovo diritto di utilizzare i dati personali generati dall'uso di un prodotto connesso o di un servizio correlato. In tali casi potrebbe essere nell'interesse dell'utente facilitare il rispetto dei requisiti di cui all'articolo 6 del regolamento (UE) 2016/679. Poiché il presente regolamento non dovrebbe ledere i diritti alla protezione dei dati degli interessati, in tali casi il titolare dei dati può dar seguito alle richieste, tra l'altro, anonimizzando i dati personali o, nel caso in cui i dati prontamente disponibili contengano dati personali di più interessati, trasmettendo solo i dati personali relativi all'utente».

Lasciando l'esaustività ai tanti lavori già offerti sulla materia[38], ciò che a noi interessa riguarda le norme inerenti l'utilizzo dei dati da parte dell'attore pubblico.

---

[37] Si veda: G. DE MINICO, *Too many rules or zero rules for the ChatGPT?*, in *BioLaw Journal – Rivista di BioDiritto*, n. 2/2023, 491-501, in particolare a p. 497 l'Autrice apre alla possibile incorporazione del GDPR in uno con l'AI Act per combattere l'eccessiva confusione normativa; T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto,* n. 1/2022, 155-164, in particolare p. 10 e ss. sul GDPR come base dell'AI Act; D. MARTIRE, *Intelligenza artificiale e Stato costituzionale*, in *Diritto pubblico*, n. 2/2022, 397-444, in particolare p. 409 e ss. sul GDPR come punto di partenza privilegiato. Si veda l'art. 2 par. 7 AI Act: «Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680, fatte salve le disposizioni di cui all'articolo 10, paragrafo 5, e all'articolo 59 del presente regolamento». Inoltre, si veda la Relazione alla Proposta di AI Act, al punto 1.2: «La proposta non pregiudica il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (direttiva (UE) 2016/680) e li integra con una serie di regole armonizzate applicabili alla progettazione, allo sviluppo e all'utilizzo di determinati sistemi di IA ad alto rischio nonché di restrizioni concernenti determinati usi dei sistemi di identificazione biometrica remota. La presente proposta integra inoltre il diritto dell'Unione in vigore in materia di non discriminazione con requisiti specifici che mirano a ridurre al minimo il rischio di discriminazione algoritmica, in particolare in relazione alla progettazione e alla qualità dei set di dati utilizzati per lo sviluppo dei sistemi di IA, integrati con obblighi relativi alle prove, alla gestione dei rischi, alla documentazione e alla sorveglianza umana durante l'intero ciclo di vita dei sistemi di IA. La presente proposta non pregiudica l'applicazione del diritto dell'Unione in materia di concorrenza».

[38] Tra i numerosi articoli sul tema: C. COLAPIETRO, *Gli algoritmi tra trasparenza e protezione dei dati personali*, in *federalismi.it (Osservatorio sulla trasparenza)*, 22.02.2023, 24, p. 158 e ss.; C. COLAPIETRO, *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *federalismi.it*, 13.04.2020, 28, p. 74 e ss.; G. DE MINICO, *Indagine conoscitiva sull'intelligenza artificiale*, Audizione al Senato del 3.12.2020, p. 5 sul *considerandum* 63 al GDPR; G. DE MINICO, *Fundamental Rights, European Digital Regulation and Algorithmic Challenge*, in *MediaLaws*, n. 1/2021, 9-38, in particolare p. 22 e ss.; G. DE MINICO, *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2021, 381-403, in particolare p. 388 sull'evoluzione della *privacy* per il tramite del GDPR; A.J. WULF and O. SEIZOV, *Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU*, in *European Business Law Review* 31, n. 4/2020, 611-640, p. 619 e ss.; G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, cit., in particolare p. 208 sui benefici apportati dal GDPR all'ecosistema informativo e p. 223 sull'Art. 15 GDPR; A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, 63-89, in particolare p. 79 e ss.

Anzitutto, l'art. 6 GDPR disciplinante le condizioni per la «liceità del trattamento» prevede al par. 1 lett. 'e' la possibilità di trattare i dati personali – senza consenso – quando «è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento». Sulla stessa scia e circa i dati personali particolarmente sensibili – come e.g. l'orientamento sessuale, religioso, politico – l'art. 9 par. 2 lett. 'g' dispone l'utilizzabilità se «il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato». Ma andiamo ancora più nel dettaglio.

I parametri fondanti le eccezioni all'utilizzo dei dati personali da parte delle Istituzioni presenti in GDPR e Reg. (UE) 2018/1725 sono: a. necessario per motivi di interesse pubblico (art. 9 par. 2 lett. g GDPR – art. 10 par. 2 lett. g Reg. (UE) 2018/1725); b. necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 20 par. 3 secondo periodo GDPR – art. 22 par. 3 secondo periodo Reg. (UE) 2018/1725); c. l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (art. 21 par. 1 GDPR – art. 23 par. 1 Reg. (UE) 2018/1725); d. qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica (art. 23 GDPR – art. 25 Reg. (UE) 2018/1725); e. a fini di ricerca scientifica o storica o a fini statistici o per finalità di archiviazione nel pubblico interesse (art. 25 parr. 3 e 4 Reg. (UE) 2018/1725 collegati agli artt. 13 e 20 par. 4 Reg. (UE) 2018/1725).

Il contenuto di questi parametri si trova declinato, per quanto concerne il nostro Paese, all'interno del d.lgs. 196/2003 (Codice Privacy – da ora CP)[39].

Circa il parametro 'a', l'art. 2-sexies CP al co. 1 prevede:

[39] DECRETO LEGISLATIVO 30 giugno 2003, n. 196: Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

«I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Il successivo co. 2 elenca poi le materie che si considerano rilevanti per l'interesse pubblico «relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri»[40].

[40] Art. 2-sexies co. 2 CP che dispone: «Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: a) accesso a documenti amministrativi e accesso civico; b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità; c) tenuta di registri pubblici relativi a beni immobili o mobili; d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli; e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato; f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari; g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche; h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo; i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale, comprese quelle di prevenzione e contrasto all'evasione fiscale; l) attività di controllo e ispettive; m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni; n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali; o) rapporti tra i soggetti pubblici e gli enti del terzo settore; p) obiezione di coscienza; q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria; r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose; s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi,

Circa i parametri 'b' e 'c', l'art. 2-undecies CP prevede limitazioni ai diritti dell'interessato di cui agli artt. da 15 a 22 GDPR qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto a determinati interessi[41]. Infatti, il co. 3 del

non autosufficienti e incapaci; t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano; u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica; v) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale; z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria; aa) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili; bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario; cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan); dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva».

[41] Art. 2-undecies CP (Limitazioni ai diritti dell'interessato): «1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto: a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio; b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive; c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione; d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria; f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ovvero

medesimo articolo prevede: «[…] L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e), f) e f-bis) […]».

Circa il parametro 'd', troviamo l'individuazione delle materie stesso nell'art 23 par. 1 GDPR (art. 25 par. 1 Reg. (UE) 2018/1725):

> «a) la sicurezza nazionale; b) la difesa; c) la sicurezza pubblica; d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale; f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g); i) la tutela dell'interessato o dei diritti e delle libertà altrui; j) l'esecuzione delle azioni civili».

La materia di cui alla lett. f trova una particolare declinazione nell'art. 2-duodecies (Limitazioni per ragioni di giustizia)[42].

Circa il parametro 'e', il CP prevede vari allegati recanti regole deontologiche per il trattamento dei dati con finalità di archiviazione[43], statistiche o di ricerca scientifica nell'ambito del sistema statistico nazionale[44] e non[45].

---

che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58».

[42] Si consulti su normattiva: art. 2-duodecies (Limitazioni per ragioni di giustizia).

[43] Consultabile su normattiva, l'allegato 2 «Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica» è stato poi modificato con Delibera del Garante n. 513 del 19 dicembre 2018, in G.U. 15 gennaio 2019, n. 12.

[44] Consultabile su normattiva, l'allegato 3 «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale» è stato poi modificato con Delibera del Garante n. 514 del 19 dicembre 2018, in G.U. 14 gennaio 2019, n. 11.

Volendo riassumere le *ratio* sottostanti a tali eccezioni, possiamo affermare che dinanzi agli interessi pubblici i diritti dei singoli alla tutela dei dati personali, anche di categoria particolare, vengono considerati "secondari" nei vari bilanciamenti di valore. Ovviamente, sempre nel rispetto di dovute garanzie sostanziali e procedimentali, tipiche della *rule of law*:

> «Per essere giustificata, una simile lesione dev'essere prevista dalla legge, deve rispettare il contenuto essenziale di detti diritti e, in applicazione del principio di proporzionalità, dev'essere necessaria e rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione, considerato il fatto che le deroghe e le limitazioni a tali diritti devono operare entro i limiti dello stretto necessario»[46].

Se il GDPR risulta essere uno strumento che offre un'elevata tutela dei diritti dell'interessato quando i suoi dati personali sono oggetto di finalità economiche – in particolare di marketing diretto – degli attori privati; sempre il GDPR (insieme al Reg. (UE) 2018/1725) apre a numerose eccezioni, adeguatamente oggetto di garanzie, per l'utilizzo dei dati personali degli interessati da parte delle Istituzioni.

3. Il Data Act

La specifica trasversalità dei dati ha condotto l'Unione a ideare internamente alla strategia digitale la «strategia europea in materia di dati»[47]. Con questa prospettiva sistemica e consapevole delle mancanze caratterizzanti la regolazione preesistente, il Legislatore

---

[45] Consultabile su normattiva, l'allegato 4 «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica» è stato poi modificato con Delibera del Garante n. 515 del 19 dicembre 2018, in G.U. 14 gennaio 2019, n. 11.

[46] CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA – DIREZIONE DELLA RICERCA E DOCUMENTAZIONE, *Scheda tematica – Protezione dei dati personali*, in *curia.europa.eu*, il 1.01.2021, 68, a p. 5 riferendosi al punto 65 della Sentenza del 9 novembre 2010 (Grande Sezione), Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662).

[47] Si veda sul sito della Commissione: strategia europea in materia di dati. Gli obiettivi sono sintetizzati nel sottotitolo della *web page* indicata: «Fare in modo che l'UE assuma il ruolo di modello per una società più autonoma grazie ai dati».

eurounitario ha articolato una folta disciplina circa *share, compete* e *use*[48] dei dati tramite principalmente DGA, DMA e DA.

La tipologia di sistema – privato e pubblico – di *governance* dei dati che si sta costruendo è qualificabile come *interdependence model*[49]. Questo nasce in contrapposizione ai modelli *independence* consolidatisi in USA e Cina,

> «dove il trattamento e la gestione dei dati risponde ad una logica verticale e centralizzata, caratterizzata da un elevato grado di indipendenza – del soggetto privato o di quello pubblico – nei confronti dei concorrenti. A tale riguardo, infatti, è possibile distinguere, da un lato, la versione statunitense orientata ad un approccio di autoregolamentazione pura che conduce al consolidamento di posizioni di dominio da parte dei soggetti che offrono servizi OTT, mentre dall'altro lato, il paradigma cinese che si caratterizza per un pesante controllo statale sulle iniziative private nell'intento di assicurare al soggetto pubblico l'accesso ad una quantità di dati più vasta»[50].

---

[48] «These three areas of focus (share, compete, use) have been fully embraced by the co-legislators. The interinstitutional negotiations on the Data Governance Act (data sharing) were finalised on 30 November 2021, only a year after the Commission made its proposal. For the Digital Markets Act (compete), both co-legislators are finalising their position. They indicated the need to go further on usage issues in the context of the Data Act proposal» a p. 1 di: *Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)* – SWD(2022) 34 final.

[49] S. TORREGIANI, *La disciplina europea dei dati: dalla protezione alla governance*, cit., p. 262. Si veda anche p. 221: «il modello oggi predominante nella data economy consiste nella concentrazione di enormi quantità di dati nei server di pochi potenti attori le cui sedi sono collocate al di fuori dell'Unione. L'accumulo di potere che deriva da siffatto metodo di elaborazione dei dati costituisce un grave pericolo sia per la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali, sia per la concorrenza nel mercato europeo. La volontà di prevenire il consolidamento dell'oligarchia dei giganti della tecnologia ha spinto, dunque, verso un modello improntato ad una logica spiccatamente redistributiva. La divisione delle funzioni e la compartecipazione di più attori economici nella formazione delle catene di valore dei dati aspira a proporsi quale alternativa "più democratica" alla centralizzazione nella raccolta e nell'analisi dei dati delle grandi piattaforme online, riducendo drasticamente le opportunità di concentrazione e, conseguentemente, la creazione di monopoli ed oligopoli». Si veda anche a pp. 271-273 circa l'approccio "nazionalista" del DGA e sull'importanza sempre maggiore dei dati non personali: lo «spazio comune europeo dei dati» è la *condicio sine qua non* per governare la tecnologia ed essere sovrani nell'era digitale.

[50] Ivi, p. 262.

La declinazione del modello europeo si trova in particolare all'interno del DGA, e si richiama ai c.d. *FAIR principles*[51]: *findable* (reperibili), *accessible* (accessibili), *interoperable* (interoperabili), *re-usable* (riutilizzabili)[52]. Il sistema di *governance* eurounitario si basa quindi su una chiara prospettiva di *data sharing*:

> «il DGA promuove un sistema qualificabile come "*interdependence model*", ispirato ad un'ottica collaborativa secondo cui differenti soggetti sono chiamati a (co)operare sulla base di una relazione di stretta interdipendenza, funzionale sia alla circolazione dei dati che alla distribuzione del potere di mercato. In tal senso, attraverso la disciplina di un'infrastruttura concepita come neutrale e aperta, il legislatore non persegue l'obiettivo dell'esclusione altrui come accade nell'*independence model*, ma favorisce l'instaurazione di rapporti di interdipendenza tra operatori, anche provenienti dall'esterno, i quali sono chiamati ad agire nel rispetto delle regole del sistema»[53].

Tale ricercata interdipendenza si declina anche per il tramite dell'*Interoperable Europe Act* che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione[54]. Sebbene sia forse controintuitivo, l'interoperabilità sistemica prevista dallo IEA

---

[51] «L'atto si ispira ai principi per la gestione e il riutilizzo dei dati che sono stati elaborati per i dati di ricerca. I principi "FAIR" per i dati stabiliscono che tali dati dovrebbero, in linea di principio, essere reperibili, accessibili, interoperabili e riutilizzabili» a p. 2 della Relazione alla Proposta di DGA.

[52] M. WILKINSON, M. DUMONTIER, I. AALBERSBERG ET AL., *The FAIR Guiding Principles for scientific data management and stewardship*, in *Scientific Data*, 2016, 9. Si veda anche: https://force11.org/info/the-fair-data-principles/.

[53] S. TORREGIANI, *La disciplina europea dei dati: dalla protezione alla governance*, cit., p. 263.

[54] Tra l'altro, tale interdipendenza è essenziale per raggiungere l'obiettivo dell'accessibilità online del 100 % dei servizi pubblici fondamentali entro il 2030 fissato dall'art. 4 par. 1 n. 4 della Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030. Si veda anche il *considerandum* 14 IEA: «Onde eliminare la frammentazione del panorama dell'interoperabilità nell'Unione, dovrebbero essere promossi una concezione comune di interoperabilità nell'Unione e un approccio olistico alle soluzioni di interoperabilità. Una cooperazione strutturata dovrebbe sostenere le misure volte a promuovere un'impostazione delle politiche pronta per il digitale e basata sulla "interoperabilità fin dalla progettazione". Dovrebbe inoltre promuovere la gestione e l'uso efficienti delle infrastrutture di servizi digitali e delle loro rispettive componenti da parte dei soggetti dell'Unione e degli enti pubblici onde consentire l'istituzione e il funzionamento di servizi pubblici sostenibili ed efficienti, con l'obiettivo di garantire l'accessibilità fino al livello amministrativo più basso». Si veda anche S. TORREGIANI, *La disciplina europea dei dati: dalla protezione alla governance*, cit., a p. 219: «L'interoperabilità è stata da tempo individuata quale strumento fondamentale per combattere la chimera dell'assenza di standard comuni per i dati in ambito

integra GDPR e Reg. (UE) 2018/1725[55] senza pregiudicarne la capacità protettiva dei dati personali[56]. Avere un unico sistema europeo, interoperabile e strutturato su una piattaforma *cloud* comune rafforza la cybersicurezza a tutela dei dati che circolano e circoleranno[57]. L'adempimento delle soluzioni indicate dall'IEA sarà svolto dai 27 Paesi membri con il coordinamento dello *Interoperable Europe Board* ex artt. 15 e ss. IEA e del portale "Europa Interoperabile" ex art. 8 IEA messo a disposizione dalla Commissione.

Il *digital market act*[58], poi, disciplina il *compete* dei dati detenuti dalle grandi piattaforme e.g assoggettando i *gatekeeper*[59] ad obblighi specifici per prevenire abusi di posizione

---

continentale: un ambiente digitale florido e dinamico non può prescindere dall'adozione di standard condivisi che permettano di rendere meno farraginoso il flusso dei dati tra i diversi anelli della catena di comunicazione».

[55] Al *considerandum* 11 IEA: «[…] Il presente regolamento integra e non pregiudica il diritto dell'Unione in materia di protezione dei dati personali e vita privata, in particolare i regolamenti (UE) 2016/679 e (UE) 2018/1725 nonché la direttiva 2002/58/CE. Nessuna disposizione del presente regolamento dovrebbe essere applicata o interpretata in modo da ridurre o limitare il diritto alla protezione dei dati personali o il diritto alla vita privata e alla riservatezza delle comunicazioni».

[56] A supporto di tali obiettivi saranno utilizzati appositi spazi di sperimentazione normativa per l'interoperabilità ex art. 11 IEA; si veda il *considerandum* 42 IEA: «[…] Il presente regolamento è volto unicamente a prevedere il trattamento dei dati personali nel contesto dello spazio di sperimentazione normativa per l'interoperabilità. Qualsiasi altro trattamento di dati personali che rientri nell'ambito di applicazione del presente regolamento richiederebbe una base giuridica distinta».

[57] Ad oggi, in Italia, una grande parte dei dati detenuti dalle varie pubbliche amministrazioni sono conservati in migliaia di singole memorie dati gestite tramite *server* altamente vulnerabili. Si veda: https://cert-agid.gov.it/news/mappatura-delle-vulnerabilita-della-pubblica-amministrazione-mediante-fonti-osint/.

[58] Si veda: G. DE MINICO, *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti*, in *federalismi.it*, n. 6/2024, 21, p. 14 e ss.

[59] La Commissione europea ha designato il 6.09.2023, per la prima volta, sei *gatekeeper* — Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft — ai sensi della legge sui mercati digitali. Si veda: https://digital-strategy.ec.europa.eu/it/news/digital-markets-act-commission-designates-six-gatekeepers. Inoltre, «con l'ordinanza del 9 febbraio 2024 nella causa T-1077/23 R, il Tribunale dell'Unione europea ha respinto la domanda, avanzata da ByteDance Ltd di sospendere provvisoriamente l'esecuzione della decisione della Commissione che la designa come gatekeeper; tale provvedimento segna, così, la prima pronuncia dei giudici di Lussemburgo in materia di applicazione del Regolamento (UE) 2022/1925 sui mercati digitali», si veda: F. TOGNATO, *Primo provvedimento del Tribunale in materia di DMA: i giudici di Lussemburgo respingono la domanda di sospensione proposta da Bytedance*, in *Eurojus.it*, il 4.03.2024.

dominante[60]. È proprio tramite questi numerosi obblighi che il DMA tutela la costruzione dell'*interdependence model* ingabbiando le grandi piattaforme *gatekeeper* – tutte extra UE – al suo rispetto.

Chiarito il sistema, è bene ritornare sull'oggetto di queto lavoro e approfondire alcune norme del *Data Act*[61] contenute nel Capo V «mettere i dati a disposizione di enti pubblici, della

[60] G. DE MINICO, *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti*, cit., p. 16: «A nostro avviso, il D.M.A. intende prevenire gli abusi di dominanza, intervenendo prima che l'illecito si consumi, e questa anticipazione della soglia della punibilità si compie nel mettere una camicia di forza all'operatore con significativo potere di mercato, scaricandogli addosso obblighi comportamentali diretti a impedire la degenerazione della sua dominanza in abuso».

[61] La Commissione ha presentato la proposta di normativa sui dati «con l'intento di garantire un'equa ripartizione del valore dei dati tra gli operatori dell'economia dei dati e di promuovere l'accesso ai dati e il relativo utilizzo. Di seguito sono sintetizzati gli obiettivi specifici della proposta.

– Facilitare l'accesso ai dati e il relativo utilizzo da parte dei consumatori e delle imprese, preservando nel contempo gli incentivi a investire in modalità di generazione del valore grazie ai dati. A tal fine sono necessari tra l'altro maggiore certezza del diritto in merito alla condivisione dei dati ottenuti o generati dall'uso di prodotti o di servizi correlati, e l'attuazione di norme che garantiscano l'equità nei contratti di condivisione dei dati. La proposta chiarisce l'applicazione alle sue disposizioni dei diritti pertinenti previsti dalla direttiva 96/9/CE relativa alla tutela giuridica delle banche di dati (direttiva sulle banche di dati).

– Prevedere che enti pubblici e istituzioni, agenzie o organismi dell'Unione possano utilizzare i dati detenuti dalle imprese in determinate situazioni in cui vi sia una necessità eccezionale di dati. Ciò riguarda principalmente le emergenze pubbliche, ma anche altre situazioni eccezionali in cui la condivisione obbligatoria dei dati tra imprese e pubbliche amministrazioni è giustificata al fine di sostenere politiche e servizi pubblici basati su dati concreti, efficaci, efficienti e orientati ai risultati.

– Facilitare il passaggio tra diversi servizi cloud ed edge. L'accesso a servizi di trattamento dei dati competitivi e interoperabili è una condizione preliminare per una economia dei dati fiorente, in cui i dati possano essere facilmente condivisi all'interno degli ecosistemi settoriali e tra di essi. Il livello di fiducia nei servizi di trattamento dei dati determina la diffusione di tali servizi tra gli utenti in tutti i settori dell'economia.

– Adottare garanzie contro il trasferimento illecito di dati senza notifica da parte dei fornitori di servizi cloud. Tale obiettivo deriva dal fatto che sono state espresse preoccupazioni in merito all'accesso illecito ai dati da parte di amministrazioni pubbliche di paesi terzi/esterni allo Spazio economico europeo (SEE). Simili garanzie dovrebbero rafforzare ulteriormente la fiducia nei servizi di trattamento dei dati che sono sempre più fondamentali per l'economia europea dei dati.

Commissione, della Banca Centrale europea e di organismi dell'Unione sulla base di necessità eccezionali» (artt. 14-22).

L'art. 14 DA impone un vero e proprio obbligo di messa a disposizione dei dati «sulla base di necessità eccezionali» alle Autorità pubbliche. L'art. 15 DA[62] ne delimita l'eccezionalità di *usage*: cosa si intende per «necessità di utilizzare determinati dati»? La norma disciplina due *species*: a. «emergenza pubblica»; b. «svolgere un compito specifico svolto nell'interesse pubblico esplicitamente previsto dalla legge».

Il caso 'a' esige il rispetto di determinate condizioni, quali: a. «i dati richiesti sono necessari per rispondere all'emergenza pubblica»; b. non possono essere ottenuti «con mezzi alternativi in modo tempestivo ed efficace a condizioni equivalenti».

– Prevedere l'elaborazione di norme di interoperabilità per il riutilizzo dei dati tra i vari settori, nel tentativo di eliminare gli ostacoli alla condivisione dei dati tra spazi comuni europei di dati specifici per settore, coerentemente con le prescrizioni di interoperabilità settoriali, e tra altri dati che non rientrano nell'ambito di uno spazio comune europeo dei dati specifico. La proposta sostiene inoltre la definizione di norme per i "contratti intelligenti", ossia programmi informatici su registri elettronici che eseguono e regolano transazioni sulla base di condizioni prestabilite. Tali programmi possono potenzialmente fornire ai titolari e ai destinatari dei dati garanzie del rispetto delle condizioni per la condivisione dei dati» a p. 3 di: *Relazione alla proposta di Data Act*.

[62] Articolo 15 «Necessità eccezionale di utilizzare i dati» dispone: «1. Una necessità eccezionale di utilizzare determinati dati ai sensi del presente capo è limitata nel tempo e nella portata e si considera esistente esclusivamente in una delle circostanze seguenti: a) se i dati richiesti sono necessari per rispondere a un'emergenza pubblica e l'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione non può ottenere tali dati con mezzi alternativi in modo tempestivo ed efficace a condizioni equivalenti; b) in circostanze non contemplate dalla lettera a) e solo nella misura in cui si tratti di dati non personali qualora: i) un ente pubblico, la Commissione, la Banca centrale europea o un organismo dell'Unione agisca sulla base del diritto dell'Unione o nazionale e abbia individuato dati specifici la cui mancanza gli impedisce di svolgere un compito specifico svolto nell'interesse pubblico esplicitamente previsto dalla legge, quali la redazione di statistiche ufficiali, la mitigazione o la ripresa dopo un'emergenza pubblica; e ii) l'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione abbia esaurito tutti gli altri mezzi a sua disposizione per ottenere tali dati, compresi, l'acquisto dei dati sul mercato ai prezzi di mercato o il ricorso a obblighi vigenti in materia di messa a disposizione dei dati oppure l'adozione di nuove misure legislative che potrebbero garantire la tempestiva disponibilità dei dati. 2. Il paragrafo 1, lettera b), non si applica alle microimprese e alle piccole imprese. 3. L'obbligo di dimostrare che l'ente pubblico non ha potuto ottenere i dati non personali acquistandoli sul mercato non si applica quando il compito specifico svolto nell'interesse pubblico è la produzione di statistiche ufficiali e quando l'acquisto di tali dati non è autorizzato dal diritto nazionale».

Il caso 'b' riguarda solo i dati non personali e si applica fuori dai casi di emergenza pubblica e non per micro o piccole imprese. L'art. 15 par. 1 lett. b DA prevede le seguenti condizioni: a. deve trattarsi di «dati specifici la cui mancanza gli impedisce di svolgere un compito specifico svolto nell'interesse pubblico esplicitamente previsto dalla legge»; b. quando «gli altri mezzi a sua disposizione per ottenere tali dati, compresi, l'acquisto dei dati sul mercato ai prezzi di mercato o il ricorso a obblighi vigenti in materia di messa a disposizione dei dati oppure l'adozione di nuove misure legislative che potrebbero garantire la tempestiva disponibilità dei dati» non siano disponibili. Si badi, ex art. 15 par. 3 DA le Autorità pubbliche sono esenti dal dimostrare di non aver trovato i dati sul mercato «quando il compito specifico svolto nell'interesse pubblico è la produzione di statistiche ufficiali e quando l'acquisto di tali dati non è autorizzato dal diritto nazionale».

Per entrambe le *species* sarà necessario presentare alle imprese una apposita «richiesta di messa a disposizione dei dati» secondo le modalità e rispettando i requisiti imposti dall'art. 17 DA; in particolare, il par. 2 alla lett. d prevede a tutela degli interessi imprenditoriali che la richiesta chiarisca il rispetto degli «obiettivi legittimi del titolare dei dati, impegnandosi a rispettare la tutela dei segreti commerciali in conformità dell'articolo 19, paragrafo 3, e tenendo conto dei costi e degli sforzi necessari per mettere a disposizione i dati»[63]. Inoltre, a tutela della *privacy* sui dati personali la successiva lett. e prevede che l'Autorità pubblica, in caso di emergenza «richiede dati personali in forma pseudominizzata e istituisce le misure tecniche e organizzative che saranno adottate per proteggere i dati». Ex art. 20 DA le imprese avranno diritto a un compenso – copertura dei costi più un margine ragionevole – ma non nel caso della necessità eccezionale di «emergenza pubblica», e qualora per la *species* 'b' «il

[63] L'art. 19 par. 3 DA prevede: «La divulgazione di segreti commerciali a un ente pubblico, alla Commissione, alla Banca centrale europea o a un organismo dell'Unione è obbligatoria solo nella misura strettamente necessaria per conseguire lo scopo di una richiesta a norma dell'articolo 15. In tali casi, il titolare dei dati o, qualora non si tratti della stessa persona, il detentore del segreto commerciale individua i dati protetti quali segreti commerciali, compresi i pertinenti metadati. L'ente pubblico, la Commissione, la Banca centrale europea o l'organismo dell'Unione adotta, prima della divulgazione di segreti commerciali, tutte le misure tecniche e organizzative necessarie e adeguate per preservare la riservatezza dei segreti commerciali, ivi compreso, se del caso, l'uso di clausole contrattuali tipo, norme tecniche e l'applicazione di codici di condotta».

compito specifico svolto nell'interesse pubblico è la produzione di statistiche ufficiali e se il diritto nazionale non consente l'acquisto di dati»[64].

Il compito di dare "contenuto" ai casi di «necessità eccezionale» – che ex art. 15 DA permettono la messa a disposizione dei dati – è affidato dal Regolamento alle Autorità competenti individuate dai singoli Stai membri, coordinate dalla Commissione e dall'EDIB che ex art. 42 lett. a DA consiglia e assiste la Commissione «nello sviluppo di una prassi coerente delle autorità competenti nell'esecuzione dei capi II, III, V e VII».

La regolamentazione dello *use* dei dati detenuti dai privati da parte delle Autorità pubbliche per l'assolvimento di compiti specifici, nonché anche di dati personali e senza particolari giustificazione nei casi di «emergenza», si inserisce nel solco dell'analisi svolta su GDPR e Reg. (UE) 2018/1725. Abbiamo visto come questi ultimi aprono a numerose eccezioni, adeguatamente oggetto di garanzie, per l'utilizzo dei dati personali degli interessati da parte delle Istituzioni. Il *Data Act* ne aggiunge altre, e queste toccano i dati raccolti e custoditi dai privati.

4. L'AI Act

La dimensione europea anche sull'*artificial intelligence* è necessaria[65]; infatti l'interesse «è quello di preservare la leadership tecnologica dell'UE e assicurare che i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione»[66]. L'AI Act vuole contribuire all'obiettivo dell'Unione di essere un *leader* mondiale nello sviluppo di un'intelligenza artificiale sicura, affidabile ed

[64] Circa l'utilizzo dei dati per finalità statistiche si veda anche l'art. 21 DA «Condivisione dei dati ottenuti nel contesto di necessità eccezionali con organismi di ricerca o istituti statistici».

[65] *Ex multis*: C. SCHEPISI, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V. FALCE (*a cura di*), *Strategia del dati e intelligenza artificiale – Verso un nuovo ordine giuridico del mercato*, Torino, G. Giappichelli Editore, 2023, 316, 53-75.

[66] A p. 1 della Relazione alla proposta di AI Act.

etica[67] garantendone i principi sin dalla progettazione[68], a differenza di Cina e USA che hanno preferito dare rilevanza per lo più alla "sicurezza"[69].

Su questa scia si è andati *step by step* verso una versione definitiva ma sempre *in fieri* del Regolamento generale sull'intelligenza artificiale. Esito di un lungo processo[70], esso prevede apposite modalità di aggiornamento e modifica[71], essenziali per adattarsi nel tempo alle novità tecnologiche inerenti l'IA[72].

---

[67] Come dichiarato dal Consiglio europeo con le Conclusioni, EUCO 13/20, 2020, p. 7.

[68] Come richiesto specificamente dal Parlamento europeo tramite la Risoluzione del 20 ottobre 2020 – e.g. ai punti 3 e 5 – recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate.

[69] La Cina con le sue misure provvisorie del 13.07.2023 per l'IA generativa mentre gli USA con l'*executive order* del 30.10.2023. Si vedano queste analisi comparative dei diversi approcci: B.C. LARSEN and S. KÜSPERT, *Regulating general-purpose AI: Areas of convergence and divergence across the EU and the US*, in *brookings.eu*, il 21 maggio 2024; I. CARDILLO, *Disciplina dell'intelligenza artificiale e intelligentizzazione della giustizia in Cina*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3/2022, 139-167; C. DJEFFAL, M.B. SIEWERT and S. WURSTER, *Role of the state and responsibility in governing artificial intelligence: a comparative analysis of AI strategies*, in *Journal of European Public Policy*, v. 29 n. 11 del 2022, 1799-1821; E. HINE and L. FLORIDI, *Artificial intelligence with American values and Chinese characteristics: a comparative analysis of American and Chinese governmental AI policies*, in *AI & SOCIETY*, published online 25/06/2022, 22; A. MALASCHINI, *Regolare l'intelligenza artificiale. Le risposte di Cina, Stati Uniti, Unione europea, Regno Unito, Russia e Italia*, in P. SEVERINO (*a cura di*), *Intelligenza artificiale, Politica, economia, diritto, tecnologia*, Roma, Luiss University Press, 2021, 104-169; J. MÖKANDER, P. JUNEJA, D. WATSON, L. FLORIDI, *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?*, in *Minds & Machines*, n. 32/2022, 751-758; H. ROBERTS et al, *Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes*, in *The Information Society*, 28/09/2022, 20.

[70] In attesa dell'applicabilità del Regolamento, la Commissione europea ha lanciato l'iniziativa *AI Pact*; questa ha l'obiettivo di incentivare le aziende ad anticipare l'adattamento alle norme così da trovarsi pronti: https://digital-strategy.ec.europa.eu/en/policies/ai-pact?utm_source=substack&utm_medium=email.

[71] Disciplinate in via generale all'art. 112 «Valutazione e riesame» prevedendo cadenze periodiche. Si veda anche nello specifico l'art. 7 «Modifiche dell'allegato III» riguardante la qualificazione dei sistemi di IA ad alto rischio.

[72] «La proposta definisce un quadro giuridico solido e flessibile. Da un lato, è completa e adeguata alle esigenze future per quanto concerne le sue scelte normative fondamentali, compresi i requisiti basati sui principi che i sistemi di IA dovrebbero soddisfare. Dall'altro, mette in atto un sistema normativo proporzionato incentrato su un approccio normativo ben definito basato sul rischio che non crea restrizioni inutili al commercio, motivo per cui l'intervento legale è adattato alle situazioni concrete nelle quali sussiste un motivo di preoccupazione

Con la versione conclusiva molti passi sono stati fatti in avanti, a partire dalla più specifica – di quella originariamente inserita nella proposta di regolamento del 2021[73] – definizione di *AI System*: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[74].

L'AI Act è stato approvato dal Parlamento europeo il 13 marzo 2024, il lungo procedimento legislativo ha prodotto con 180 *consideranda*, 113 articoli e 13 allegati la prima – al mondo – «legge sull'intelligenza artificiale»[75] di tipo generale; è ricchissimo di norme il cui approfondimento può rispondere a sofisticate curiosità di ricerca[76], quelle concernenti questo

---

giustificato o nelle quali tale preoccupazione può essere ragionevolmente prevista nel prossimo futuro. Allo stesso tempo il quadro giuridico comprende meccanismi flessibili che fanno sì che esso possa essere adeguato dinamicamente all'evoluzione della tecnologia e all'emergere di nuove situazioni di preoccupazione» a p. 3 della Relazione alla proposta di AI Act.

[73] L'art. 3 punto 1 della Proposta di AI Act prevedeva questa definizione di "sistema di intelligenza artificiale" (sistema di IA): «software sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono».

[74] Prevista all'art. 3 punto 1 AI Act. In realtà, si è ripresa la definizione offerta dall'OECD Recommendation of the Council on Artificial Intelligence aggiungendo tra gli *output* la produzione di "contenuti", includendo quindi i sistemi di intelligenza artificiale generativa. Definizione «il cui pregio è quello di aver tratteggiato i contorni della figura senza bloccarla in uno schema blindato, che ne impedirebbe la porosità alle future innovazioni tecniche» in G. DE MINICO, *Giustizia e intelligenza artificiale: un equilibrio mutevole*, cit., p. 86.

[75] Così è stato scelto di qualificare il Regolamento all'interno della sua rubrica ufficiale. Tra gli articoli che affrontano più questioni inerenti l'AI Act: O. BAKINER, *Pluralistic sociotechnical imaginaries in Artificial Intelligence (AI) law: the case of the European Union's AI Act*, in *Law, Innovation and Technology*, 14.08.2023, 26; J. LAUX, S. WACHTER and B. MITTELSTADT, *Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act*, cit.; J. LAUX, S. WACHTER and B. MITTELSTADT, *Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and the Acceptability of Risk*, cit.; A.J. WULF and O. SEIZOV, *Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU*, cit.

[76] Il tema più di frontiera riguarda senz'altro il Capo V (artt. 51-56) su gli «General Purpose AI Models». Si vedano: G. DE MINICO, *Too many rules or zero rules for the ChatGPT?*, cit. Si veda anche: S.A. YANG and A.H. ZHANG, *The Case for Regulating Generative AI Through Common Law*, in *Project Syndicate*, il 15.02.2024. Nell'iter legislativo alcune aziende hanno creato non pochi problemi, tuttavia è stato correttamente deciso di proseguire

scritto riguardano il Capo VI circa le «Misure a sostegno dell'innovazione» (artt. 57-63): in particolare gli spazi di sperimentazione normativa[77] per lo sviluppo di determinati sistemi di IA nell'interesse pubblico ex art. 59 AI Act. Prima di focalizzarci su quest'ultima norma, è essenziale però offrire una panoramica del Capo in oggetto.

Gli spazi di sperimentazione normativa sono una misura fondamentale a sostegno dell'innovazione[78], essi

> «garantiscono un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i potenziali fornitori e l'autorità competente. Tali spazi di sperimentazione normativa possono comprendere prove in condizioni reali soggette a controllo nell'ambito dello spazio di sperimentazione»[79].

---

sulla direzione di una normazione comprensiva anche dei GPAI Models. Considerando la prevedibile emigrazione verso gli USA di alcuni attori europei come Mistral AI in partnership con Microsoft (vedi su kaizenner.eu) la scelta presa è stata giusta.

[77] *Ex multis*: T. BUOCZ, S. PFOTENHAUER & I. EISENBERGER, *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, in *Law, Innovation and Technology*, 18.08.2023, 34; G. LO SAPIO, *Il regolatore alle prese con le tecnologie emergenti. La regulatory sandbox tra principi dell'attività amministrativa e rischio di illusione normativa*, in *federalismi.it*, n. 30/2022, 88-112; A. MERLINO, *Il regulatory sandbox e la teoria delle fonti*, in *Diritto Pubblico Europeo Rassegna Online*, n. 1/2022, 111-127.; M.T. PARACAMPO, *Il percorso evolutivo ed espansivo delle regulatory sandboxes da FinTech ai nuovi lidi operativi del prossimo futuro*, in *federalismi.it*, n. 18/2022, 207-232, in particolare p. 224 e ss. sull'AI Act; D. ZETZSCHE, R. BUCKLEY, J. BARBERIS and D. ARNER, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, in *Fordham Journal of Corporate & Financial Law*, n. 23/2017, 31-103.

Definizione ex art. 3 punto 55 AI Act di "spazio di sperimentazione normativa per l'IA": «un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare».

[78] Una storia di successo è rappresentata dagli spazi di sperimentazione normativa sviluppati e costantemente operanti nel campo *Fintech*, si veda *ex multis*: M.T. PARACAMPO, *Il percorso evolutivo ed espansivo delle regulatory sandboxes da FinTech ai nuovi lidi operativi del prossimo futuro*, cit.

[79] Recita così l'art. 57 par. 5 AI Act. Inoltre, il par. 9 del medesimo articolo individua cinque importanti finalità delle *AI regulatory sandbox*: «L'istituzione di spazi di sperimentazione normativa per l'IA mira a contribuire ai seguenti obiettivi: a) migliorare la certezza del diritto al fine di conseguire la conformità normativa al presente

Le modalità di accesso e utilizzo delle *AI regulatory sandbox* saranno determinate con appositi atti di esecuzione che ex art. 58 par. 1 AI Act verranno emessi dalla Commissione; questi disciplineranno: «a) criteri di ammissibilità e selezione per la partecipazione allo spazio di sperimentazione normativa per l'IA; b) procedure per la domanda, la partecipazione, il monitoraggio, l'uscita dallo spazio di sperimentazione normativa per l'IA e la sua cessazione, compresi il piano dello spazio di sperimentazione e la relazione di uscita; c) i termini e le condizioni applicabili ai partecipanti». Tali atti di esecuzione dovranno garantire le condizioni e gli obiettivi indicati nel successivo par. 2[80].

---

regolamento o, se del caso, ad altre normative dell'Unione e nazionali applicabili; b) sostenere la condivisione delle migliori pratiche attraverso la cooperazione con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA; c) promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA; d) contribuire all'apprendimento normativo basato su dati concreti; e) agevolare e accelerare l'accesso al mercato dell'Unione per i sistemi di IA, in particolare se forniti dalle PMI, comprese le start-up».

[80] Che dispone: «Gli atti di esecuzione di cui al paragrafo 1 garantiscono quanto segue: a) gli spazi di sperimentazione normativa per l'IA sono aperti a qualsiasi potenziale fornitore richiedente di un sistema di IA che soddisfi criteri di ammissibilità e selezione trasparenti ed equi, e le autorità nazionali competenti informano i richiedenti della loro decisione entro tre mesi dalla domanda; b) gli spazi di sperimentazione normativa consentono un accesso ampio e paritario e tengono il passo con la domanda di partecipazione; i potenziali fornitori possono anche presentare domande in partenariato con gli utenti e con altri terzi interessati; c) le modalità dettagliate e le condizioni relative agli spazi di sperimentazione normativa per l'IA sostengono la flessibilità, nella massima misura possibile, affinché le autorità nazionali competenti istituiscano e gestiscano i loro spazi di sperimentazione normativa per l'IA; d) l'accesso agli spazi di sperimentazione normativa per l'IA è gratuito per le PMI, comprese le start-up, fatti salvi i costi straordinari che le autorità nazionali competenti possono recuperare in maniera equa e proporzionata; e) agevolano i potenziali fornitori, attraverso i risultati dell'apprendimento degli spazi di sperimentazione normativa per l'IA, nel conformarsi agli obblighi di valutazione della conformità di cui al presente regolamento e nell'applicazione volontaria dei codici di condotta di cui all'articolo 95; f) gli spazi di sperimentazione normativa per l'IA facilitano il coinvolgimento di altri attori pertinenti nell'ambito dell'ecosistema dell'IA, quali organismi notificati e organizzazioni di normazione, PMI, start-up, imprese, innovatori, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione e poli europei dell'innovazione digitale, centri di eccellenza e singoli ricercatori, al fine di consentire e facilitare la cooperazione con i settori pubblico e privato; g) le procedure, i processi e i requisiti amministrativi per l'applicazione, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione per l'IA sono semplici, facilmente intelligibili, comunicati chiaramente per agevolare la partecipazione delle PMI, comprese le start-up, con capacità giuridiche e amministrative limitate e sono razionalizzati in tutta l'Unione, al fine di evitare la frammentazione e la partecipazione a uno spazio di sperimentazione normativa per l'IA istituito da uno Stato membro o dal Garante europeo della protezione dei dati è reciprocamente e uniformemente riconosciuta e

Le *AI regulatory sandbox* sono distinte dall'altra misura a sostegno dell'innovazione previste dal Capo VI dell'AI Act: le prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA ex artt. 60-61 AI Act. Anche in ordine a queste misure saranno essenziali gli atti di esecuzione della Commissione che regoleranno tutti i requisiti e gli elementi specifici dei «piani di prova» necessari per rispettare le condizioni dell'AI Act, in particolare quella prevista ex art. 60 par. 5 AI Act:

> «Qualsiasi soggetto delle prove in condizioni reali, o il suo rappresentante legale designato, a seconda dei casi, può, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione, ritirarsi dalle prove in qualsiasi momento revocando il proprio consenso informato e può chiedere la cancellazione immediata e permanente dei propri dati personali. La revoca del consenso informato non pregiudica la liceità o la validità delle attività già svolte».

Le modalità di richiesta e concessione del consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA sono disciplinate dall'art. 61 AI Act[81].

---

produce gli stessi effetti giuridici nell'intera Unione; h) la partecipazione allo spazio di sperimentazione normativa per l'IA è limitata a un periodo adeguato alla complessità e alla portata del progetto, che può essere prorogato dall'autorità nazionale competente; i) gli spazi di sperimentazione normativa per l'IA agevolano lo sviluppo di strumenti e infrastrutture per la sperimentazione, l'analisi comparativa, la valutazione e la spiegazione delle dimensioni dei sistemi di IA pertinenti per l'apprendimento normativo, quali l'accuratezza, la robustezza e la cibersicurezza, nonché le misure per attenuare i rischi per i diritti fondamentali e la società in generale».

[81] Che dispone: «1. Ai fini delle prove in condizioni reali di cui all'articolo 60, il consenso informato dato liberamente dai soggetti delle prove è ottenuto prima della loro partecipazione a tali prove e dopo che sono stati debitamente informati con indicazioni concise, chiare, pertinenti e comprensibili riguardanti: a) la natura e gli obiettivi delle prove in condizioni reali e i possibili disagi che possono essere connessi alla loro partecipazione; b) le condizioni alle quali devono essere effettuate le prove in condizioni reali, compresa la durata prevista della partecipazione del soggetto o dei soggetti; c) i loro diritti e le garanzie riconosciute al soggetto in relazione alla loro partecipazione, in particolare il loro diritto di rifiutarsi di partecipare e il diritto di ritirarsi dalle prove in condizioni reali in qualsiasi momento, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione; d) le modalità per richiedere che le previsioni, raccomandazioni o decisioni del sistema di IA siano ignorate o ribaltate; e) il numero di identificazione unico a livello dell'Unione delle prove in condizioni reali conformemente all'articolo 60, paragrafo 4, lettera c), e i dati di contatto del fornitore o del suo rappresentante legale da cui è possibile ottenere ulteriori informazioni. 2. Il consenso informato è datato e documentato e una copia è consegnata ai soggetti delle prove o al loro rappresentante legale».

L'AI Act fissa con sufficiente chiarezza il regime delle responsabilità per eventuali danni provocati dalla sperimentazione interna o esterna alle *AI regulatory sandbox*[82], oltre ad attribuire alle Autorità di controllo necessari poteri e competenze ex artt. 76 e 77 AI Act.

Possiamo concludere questa panoramica affermando che il Legislatore eurounitario abbia fissato con adeguata attenzione principi e condizioni di queste importanti misure a sostegno dell'innovazione; tuttavia, la nostra analisi non può essere completa, data l'ingente delega affidata alla Commissione ed in particolare all'AI Office per l'elaborazione degli atti di esecuzione implementativi degli articoli spesso al più "enunciativi" dell'AI Act.

Passando alle norme di nostro particolare interesse, anzitutto, l'art. 57 par. 3 AI Act riconosce un potere particolare all'EDPS: «Il Garante europeo della protezione dei dati può inoltre istituire uno spazio di sperimentazione normativa per l'IA per le istituzioni, gli organi e gli organismi dell'Unione e può esercitare i ruoli e i compiti delle autorità nazionali competenti conformemente al presente capo». Tale possibilità sarà con alta probabilità

[82] Responsabilità previste in forma attenuata a carico degli sviluppatori ex art. 57 parr. 11-12 AI Act: «11. Gli spazi di sperimentazione normativa per l'IA non pregiudicano i poteri correttivi o di controllo delle autorità competenti che controllano gli spazi di sperimentazione, anche a livello regionale o locale. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi di IA comporta adeguate misure di attenuazione. Le autorità nazionali competenti hanno il potere di sospendere, in via temporanea o permanente, il processo di prova o la partecipazione allo spazio di sperimentazione, se non è possibile un'attenuazione efficace, e informano l'ufficio per l'IA di tale decisione. Le autorità nazionali competenti esercitano i loro poteri di controllo entro i limiti della normativa pertinente, utilizzando i loro poteri discrezionali nell'attuazione delle disposizioni giuridiche per quanto riguarda uno specifico progetto di spazio di sperimentazione per l'IA, con l'obiettivo di sostenere l'innovazione nell'IA nell'Unione. 12. I fornitori e i potenziali fornitori partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi della normativa applicabile dell'Unione e nazionale in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione. Tuttavia, a condizione che i potenziali fornitori rispettino il piano specifico e i termini e le condizioni di partecipazione e seguano in buona fede gli orientamenti forniti dall'autorità nazionale competente, quest'ultima non infligge alcuna sanzione amministrativa in caso di violazione del presente regolamento. Nella misura in cui altre autorità competenti responsabili di altre normative dell'Unione e nazionali abbiano partecipato attivamente al controllo del sistema di IA nello spazio di sperimentazione e abbiano fornito orientamenti ai fini della conformità, nessuna sanzione amministrativa pecuniaria è inflitta in relazione a tali normative».

inverata dall'EDPS che con la sua Opinion 44/2023 ha accolto con benevolenza la previsione di apposite *AI regulatory sandbox*[83].

L'art. 59 AI Act apre ad un regime d'eccezione per i sistemi di IA sviluppati nell'interesse pubblico. Sono numerose le condizioni ex art. 59 par. 1 lett. a-j AI Act[84] che cumulativamente devono sussistere per consentire l'utilizzo dei dati personali «ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione». Anzitutto, ex lett. 'b' i dati personali trattati devono essere necessari «per il rispetto di uno o più dei requisiti di cui al capo III, sezione 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento di dati anonimizzati, sintetici o di altri dati non personali» ed ex lett. 'a' deve sussistere un interesse pubblico rilevante quale:

> «i) la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari; ii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente, la tutela della biodiversità, la protezione contro l'inquinamento, le misure per la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi; iii) la sostenibilità energetica; iv) la sicurezza e la resilienza dei sistemi di trasporto e della mobilità, delle infrastrutture critiche e delle reti; v) l'efficienza e la qualità della pubblica amministrazione e dei servizi pubblici».

A tutela di tali dati personali devono essere garantiti, ex lett. 'c' appositi «meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del Reg. (UE) 2016/679 e all'articolo 39 del Reg. (UE) 2018/1725 durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento», nonché ex lett. 'd' «un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo del potenziale fornitore e solo le persone autorizzate hanno accesso a tali dati», un ambiente di trattamento in cui i dati personali possono essere protetti ex lett. 'g' «mediante adeguate misure tecniche e organizzative e cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali».

---

[83] Consultabile al link https://www.edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf, p. 18 e ss.

[84] Da ora ci riferiremo a tali lettere.

I dati personali trattati non potranno essere condivisi ex lett. 'e' dai fornitori se creati all'interno dello «spazio di sperimentazione», mentre sempre ex lett. 'e', nel rispetto del diritto dell'Unione potranno essere condivisi se raccolti esternamente. Ogni attività od evento avvenuto durante la sperimentazione dovrà essere appositamente registrato e conservato; in particolare ex lett. 'h' «i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione, salvo diversa disposizione del diritto dell'Unione o nazionale». Inoltre, la lett. 'i' prevede che «una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica di cui all'allegato IV».

Un'ulteriore tutela prevista dall'art. 59 par. 1 è indicata dalla lett. 'j' che impone un dovere di pubblicità: «una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito web delle autorità competenti; tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo».

Infine, tramite una enunciazione descrittiva e omnicomprensiva delle varie possibilità, la lett. 'f' dispone: «il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati né incide sull'applicazione dei loro diritti sanciti dal diritto dell'Unione in materia di protezione dei dati personali».

Sebbene tutte queste condizioni si possano considerare accettabili e utili per la difesa dei dati personali, subito dopo, al par. 3 l'art. 59 prevede al secondo periodo possibili regimi estensivi: «Il paragrafo 1 lascia impregiudicato […] il diritto dell'Unione o nazionale che stabilisce la base per il trattamento dei dati personali necessario ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi o qualsiasi altra base giuridica, conformemente al diritto dell'Unione in materia di protezione dei dati personali». L'estensione delle finalità di utilizzo ha come limite la disciplina preesistente, la quale – come abbiamo evidenziato al paragrafo 2 – permette l'utilizzo dei dati personali per il perseguimento di moltissime finalità di interesse pubblico.

Ad summa, fermi i limiti veri e propri sanciti con le pratiche vietate definite ex art 5 AI Act[85], la *ratio* sottesa all'art. 59 AI Act accompagna e conferma l'equilibrio Autorità-cittadino della disciplina sancita con GDPR e Reg. (UE) 2018/1725. Anche l'*Artificial Intelligence Act* apre alla possibilità di utilizzo di dati personali ed IA per il perseguimento dei più svariati *telos* pubblici nell'esercizio dei poteri statali.

5. Conclusioni

Tramite l'analisi delle principali norme di rilievo concernenti la strategia digitale europea, abbiamo provato in questo scritto a identificare l'attuale cornice giuridica sull'utilizzo dei dati da parte delle Autorità. Possiamo affermare che dinanzi agli interessi pubblici – ovviamente, sempre nel rispetto di dovute garanzie sostanziali e procedimentali, tipiche della *rule of law* e sancite per prima dalla sentenza *Volker und Markus*[86] – i diritti dei singoli alla tutela dei dati personali, anche di categoria particolare, sono considerati "secondari" nei vari bilanciamenti di valore.

Se il GDPR risulta essere uno strumento che offre una elevata tutela dei diritti dell'interessato quando i suoi dati personali sono oggetto di finalità economiche, sempre il GDPR (insieme al Reg. (UE) 2018/1725) apre a numerose eccezioni, adeguatamente oggetto di garanzie, per l'utilizzo dei dati personali da parte delle Istituzioni. La regolamentazione prevista dal *Data Act* dello *use* dei dati detenuti dai privati da parte delle Autorità pubbliche per l'assolvimento di compiti specifici, nonché anche di dati personali e senza particolari giustificazione nei casi di «emergenza», si inserisce nel solco delle eccezioni previste da GDPR

[85] Sull'argomento si vedano, *ex multis*: R.J. NEUWIRTH, *Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)*, in *Computer Law & Security Review*, Volume 48, April 2023, 14; M. VEALE and F. BORGESIUS ZUIDERVEEN, *Demystifying the Draft EU Artificial Intelligence Act!*, in *Computer Law Review International*, n. 4/2021, 97-112, p. 98 e ss.; D. MARTIRE, *Intelligenza artificiale e Stato costituzionale*, cit., p. 426; T. CHRISTAKIS and A. LODIE, *The Conseil d'Etat Finds the Use of Facial Recognition by Law Enforcement Agencies to Support Criminal Investigations "Strictly Necessary" and Proportional*, in *European Review of Digital Administration & Law – ERDAL*, Volume 3, Issue 1, 2022, 159-165; G. MOBILIO, *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico – Osservazioni a partire dal caso Glukhin c. Russia*, in *DPCE online*, n. 1/2024, 695-705.

[86] Si riveda la nota n. 46.

e Reg. (UE) 2018/1725. Anche l'*Artificial Intelligence Act* – e.g. ex art. 59 AI Act – apre alla possibilità di utilizzo di dati personali ed intelligenza artificiale per il perseguimento dei più svariati fini pubblici nell'esercizio dei poteri statali. È evidente un certo *favor* per l'utilizzo dei dati e degli *AI System* da parte dell'attore pubblico.

Si badi, ciò non deve spaventare; sono numerosi i casi in cui per obiettivi collettivi interessi dei singoli cedono, nel caso dell'utilizzo di dati ed IA serve però chiarire con fermezza il *telos*. All'interno di uno Stato sociale di diritto questo non può che individuarsi nella rimozione degli «ostacoli di ordine economico e sociale, che, limitando di fatto l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese»[87]. E ciò, in via sintetica, si declina nel miglioramento in qualità delle funzioni statali[88]; in particolare nell'erogazione delle prestazioni essenziali ai diritti sociali, costosi dal punto di vista economico.

L'utilizzo dei dati non può che essere messo in atto dalle Istituzioni per perseguire gli obiettivi di miglioramento della democrazia; abbiamo il compito di rafforzarla e di renderla sempre più capace di rispondere ai bisogni dei cittadini[89].

---

[87] Così il quasi "poetico" art. 3 co. 2 Cost. Per una analisi approfondita del principio di eguaglianza si veda: A. D'ALOIA, *Eguaglianza. Paradigmi e adattamenti di un principio 'sconfinato'*, in *Rivista AIC*, n. 4/2021, 17-102. «In conclusione, è lo stesso dato positivo a segnalare che la sovranità popolare era un obiettivo, più che una realtà, e l'unità di fondo dello Stato doveva essere perfezionata con il superamento effettivo delle disuguaglianze» in M.F. DE TULLIO, *Uguaglianza sostanziale e nuove dimensioni della partecipazione politica*, Tesi di dottorato, a.a. 2017/2018, UNINA Federico II, 395, p. 19.

[88] I nostri sistemi fondati sullo Stato di diritto sono in seria difficoltà, fra tutti: S. ISSACHAROFF, *Democracy' Deficits*, in *Nellco Legal Scholarship Repository*, Working Papers no. 9, 2017, 32; S. CASSESE, *Che cosa resta dell'amministrazione pubblica?*, in *Rivista trimestrale di diritto pubblico*, n. 1/2019, 11.

[89] In una conferenza stampa da Presidente del Consiglio dei Ministri, Mario Draghi: «Il populismo si sconfigge con un'azione di governo che risponda ai bisogni dei cittadini» il 30 giugno 2022: https://www.ilfoglio.it/politica/2022/06/30/video/draghi-al-foglio-il-populismo-si-sconfigge-con-l-azione-di-governo--4175635/ . «Il problema per la politica che sfida il populismo è il modo attraverso cui riattivare la fiducia [...] cioè il modo per rimettere in piedi la funzione direttiva delle élite. Come si fa a interpretare il disagio sociale senza cedere alle sue tossine, cioè senza appiattirsi su un'istanza di risarcimento? Come fa la delega a rimettersi al centro di un sistema sociale che a grande maggioranza la ripudia? In una battuta, come si torna a essere popolari senza essere populisti?» in A. BARBANO, *Le dieci bugie – Buone ragioni per combattere il populismo*, Milano, Mondadori, 2019, 185, p. 15.

Tuttavia, negli *Act* eurounitari non si va al di là di una implicita direzione[90]. Non basta occuparsi del mercato digitale europeo[91] o prevedere impliciti *favor*, serve un ulteriore passo. Come utilizzano i privati i *big data as the new oil*[92] per lo sviluppo delle loro attività, nello stesso modo può e deve fare lo Stato per attuare i compiti della Repubblica, e le Istituzioni europee per il futuro dell'Unione.

---

[90] Si veda e.g. il *considerandum* 16 al DGA: «Al fine di facilitare e incoraggiare l'utilizzo dei dati detenuti da enti pubblici a fini di ricerca scientifica, gli enti pubblici sono incoraggiati a sviluppare un approccio armonizzato e processi armonizzati intesi a rendere tali dati facilmente accessibili a fini di ricerca scientifica nell'interesse pubblico. Ciò potrebbe comportare, tra l'altro, la creazione di procedure amministrative semplificate, la formattazione standardizzata dei dati, metadati informativi sulle scelte metodologiche e di raccolta dei dati e campi di dati standardizzati che consentano la facile integrazione di serie di dati provenienti da diverse fonti di dati del settore pubblico, se necessario ai fini dell'analisi. L'obiettivo di tali pratiche dovrebbe essere la promozione dei dati finanziati e prodotti con fondi pubblici a fini di ricerca scientifica, conformemente al principio "il più aperto possibile, chiuso il tanto necessario"».

[91] Una interessante direzione è offerta dalla proposta di E. LETTA, *Much more than a market,* cit., a p. 7 circa una *Fifth Freedom*: «Towards the end of his term, Jacques Delors hinted at the necessity of exploring a new dimension for the Single Market. One potential avenue for this exploration lies in the addition of a fifth freedom to the existing four, to enhance research, innovation and education in the Single Market. The fifth freedom entails embedding research and innovation drivers at the core of the Single Market, thereby fostering an ecosystem where knowledge diffusion propels both economic vitality, societal advancement and cultural enlightenment. Significant progress was achieved in the past legislature in this realm with the approval of the Digital Market Act, the Digital Services Act, the AI Act, the Data Act and the Data Governance Act, crucial steps towards the development of a modern and effective digital strategy and technological autonomy. The fifth freedom could come to complement this framework to catalyse advancements in areas such as R&D, data utilisation, competences, AI, Quantum Computing, Biotech, Biorobotics, and Space, among others. Such fields could greatly benefit from the inclusion of the fifth freedom within the Single Market framework, the freedom of investigating, exploring and creating for the benefit of humankind without disciplinary or artificial borders and limitations. This is related to the freedom of contributing to address societal challenges, such as climate change and biodiversity losses and their impact on the planet, humans and cultural heritage». Si veda anche questo *paper: Make it Simple: Our blueprint for a more innovative Europe*, pubblicato dal nuovo *Innovation Club* fondato da Germania, Estonia, Lettonia e Lituania il 21 maggio 2024 su *politico.eu*.

[92] Si veda questo articolo del *The Economist*: *The world's most valuable resource is no longer oil, but data*.

Bisogna promuovere un esplicito cambio di prospettiva: non solo come difendere i dati dei cittadini[93], ma anche come e perché normare[94], governare[95] e decidere[96] con le nuove tecnologie[97]. Un primo passo verso questa direzione potrebbe essere la "codificazione" – appositamente organizzata dal Legislatore eurounitario – della disciplina inerente l'attore istituzionale; fare chiarezza in un unico regolamento – e non in più articoli sparsi nei vari *Act* – produrrebbe certezza del diritto, efficientamento dell'agire pubblico e miglioramento delle condizioni di competitività per le nostre imprese.

---

[93] E farlo nel miglior modo possibile, tra gli altri: G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, cit.

[94] Si veda: N. MACCABIANI, *Tra Nudge-Regulation e Technological Management: "Orientamenti" Costituzionali*, in *Osservatoriosullefonti.it*, n. 3/2023, 89-121, in particolare il sintetico e chiaro *incipit* a p. 90 e ss.: «Sono molteplici le sollecitazioni esogene che possono provocare trasformazioni nel tradizionale modo di intendere il diritto. La trasformazione può senz'altro e anzitutto essere di natura contenutistica, quale evoluzione dell'ordinamento giuridico finalizzata a tenere il passo con gli sviluppi economici, sociali, scientifici e tecnologici, per poterli meglio "governare". Ciò porta a testare la "resilienza" delle categorie giuridiche rispetto alle sopravvenute "innovazioni", per elaborarne di nuove nell'eventualità le esistenti si rivelino inadeguate. La trasformazione può poi riguardare il "modo" di "fare diritto", quindi le tecniche normative o regolatorie. Così, con le leggi *science-based*, il regolatore pubblico vincola l'ambito di esercizio della propria discrezionalità legislativa alle evidenze rese da un'istruttoria comprensiva di acquisizioni scientifiche». Si veda anche: P.F. BRESCIANI e M. PALMIRANI, *Constitutional Opportunities and Risks of AI in the law-making process*, in *federalismi.it*, il 24.01.2024, 18.

[95] Si veda: K.N. METCALF, *e-Governance and Good Administration: Examples from Estonia*, in *European Review of Digital Administration & Law - ERDAL*, Volume 3, Issue 1, 2022, 73-82.

[96] *Ex multis*: P. ZUDDAS, *Pregiudizi digitali e principio di precauzione*, in *Consulta online*, n. 2/2020, 408-425; A. NAPOLITANO, *Riflessioni sul ruolo del principio di precauzione nel processo decisionale delle pubbliche amministrazioni*, in *Diritto Pubblico Europeo Rassegna online*, n. 1/2019, 203-225.

[97] È da non dimenticare questo monito: «What is our human project for the digital age? Looking at our present backwards – that is, from a future perspective – this is the time in history when we shall be seen to have laid down the foundation for our mature information societies. We shall be judged by the quality of our work» in L. FLORIDI, *Soft ethics, the governance of the digital and the General Data Protection Regulation*, in *Royal Society (Philosophical Transactions A)*, 20/07/2018, p. 2.

Bibliografia

ALMADA M. and RADU A., *The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy*, in *German Law Journal*, 2024, 1-18.

BARBANO A., *Le dieci bugie – Buone ragioni per combattere il populismo*, Milano, Mondadori, 2019, 185.

BORGHESE M., *Mercato unico digitale: la strategia europea dei dati e le 2 velocità*, in *ilSole24Ore*, il 22.12.2023.

BRADFORD A., *The Brussels Effect – How the European Union Rules the World*, New York, Oxford University Press, 2020, 404.

BRESCIANI P.F. e PALMIRANI M., *Constitutional Opportunities and Risks of AI in the law-making process*, in *federalismi.it*, il 24.01.2024, 18.

BUOCZ T., PFOTENHAUER S. & EISENBERGER I., *Regulatory sandboxes in the AI Act: reconciling innovation and safety?*, in *Law, Innovation and Technology*, 18.08.2023, 34.

CALZOLAIO S., *Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati*, in *Rivista italiana di informatica e diritto*, n. 1/2021, 5-9.

CARDILLO I., *Disciplina dell'intelligenza artificiale e intelligentizzazione della giustizia in Cina*, in *BioLaw Journal – Rivista di BioDiritto*, n. 3/2022, 139-167.

CASADEI T., *Il senso del 'limite' – Montesquieu nella riflessione di Hannah Arendt*, in FELICE D. (*a cura di*), *Montesquieu e i suoi interpreti*, Pisa, Ets, 2005, tomo II, 805-838.

CASSESE S., *Che cosa resta dell'amministrazione pubblica?*, in *Rivista trimestrale di diritto pubblico*, n. 1/2019, 11.

CHANDER A. e UYÊN P.L., *Data Nationalism*, in *Emory Law Journal*, vol. n. 64/2015, 677-740.

CHRISTAKIS T. and LODIE A., *The Conseil d'Etat Finds the Use of Facial Recognition by Law Enforcement Agencies to Support Criminal Investigations "Strictly Necessary" and Proportional*, in *European Review of Digital Administration & Law – Erdal*, Volume 3, Issue 1, 2022, 159-165.

COLAPIETRO C., *Gli algoritmi tra trasparenza e protezione dei dati personali*, in *federalismi.it (Osservatorio sulla trasparenza)*, 22.02.2023, 24.

ID., *Il complesso bilanciamento tra il principio di trasparenza e il diritto alla privacy: la disciplina delle diverse forme di accesso e degli obblighi di pubblicazione*, in *federalismi.it*, 13.04.2020, 28.

D'ALOIA A., *Eguaglianza. Paradigmi e adattamenti di un principio 'sconfinato'*, in *Rivista AIC*, n. 4/2021, 17-102.

DATEN ETHIK KOMMISSION, *Opinion of the Data Ethics Commission – Executive Summary*, Berlino, Ottobre 2019, 31

DE MINICO G., *Giustizia e intelligenza artificiale: un equilibrio mutevole*, in *Rivista AIC*, n. 2/2024, 85-108.

ID., *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti*, in *federalismi.it*, n. 6/2024, 21.

ID., *Too many rules or zero rules for the ChatGPT?*, in *BioLaw Journal – Rivista di BioDiritto*, n. 2/2023, 491-501.

ID., *Fundamental Rights, European Digital Regulation and Algorithmic Challenge*, in *MediaLaws*, n. 1/2021, 9-38.

ID., *Towards an "Algorithm Constitutional by Design"*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2021, 381-403.

ID., *Indagine conoscitiva sull'intelligenza artificiale*, Audizione al Senato del 3.12.2020.

DE TULLIO M.F., *Uguaglianza sostanziale e nuove dimensioni della partecipazione politica*, Tesi di dottorato, a.a. 2017/2018, UNINA Federico II, 395.

DELLA PORTA M.R. e SALERNO D., *RAPPORTO I-COM IA, gravi ritardi per Europa e Italia: lo dicono i dati*, in *Agenda Digitale*, il 6.11.2023.

DJEFFAL C., SIEWERT M.B. and WURSTER S., *Role of the state and responsibility in governing artificial intelligence: a comparative analysis of AI strategies*, in *Journal of European Public Policy*, v. 29 n. 11 del 2022, 1799-1821.

DOMINICI G., *Intelligenza artificiale nella Pa: come gestire al meglio una trasformazione epocale partendo dalle persone*, in *ilSole24Ore*, il 22.03.2024.

DRAGHI D., *Intervento alla High-Level Conference on the European Pillar of Social Rights*, a La Hulpe (Belgio), il 16 aprile 2024, pubblicato in italiano in *Rivista Eurojus*, n. 2/2024, 274-279.

EKELUND H., *Why there will be plenty of jobs in the future — even with artificial intelligence*, in *WEForum.org*, il 26.02.2024.

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments*, del 23.10.2023.

FLORIDI L., *Soft ethics, the governance of the digital and the General Data Protection Regulation*, in *Royal Society (Philosophical Transactions A)*, 20/07/2018.

FROSINI T.E., *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2022, 155-164.

IANNUZZI A., *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'Intelligenza Artificiale*, in *Studi parlamentari e di politica costituzionale*, n. 1/2021, 31-52.

ISSACHAROFF S., *Democracy' Deficits*, in *Nellco Legal Scholarship Repository*, Working Papers no. 9, 2017, 32.

KISSINGER H., *World Order*, trad. it. *Ordine mondiale*, Milano, Mondadori, 2015, 405.

LAUX J., WACHTER S. and MITTELSTADT B., *Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act*, in *Computer Law & Security Review*, n. 53/2024, 11.

ID., *Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and the Acceptability of Risk*, in *Regulation & Governance*, 02/2023, 34.

LETTA E., *Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens*, il 18.04.2024.

LO SAPIO G., *Il regolatore alle prese con le tecnologie emergenti. La regulatory sandbox tra principi dell'attività amministrativa e rischio di illusione normativa*, in *federalismi.it*, n. 30/2022, 88-112.

MACCABIANI N., *Tra Nudge-Regulation e Technological Management: "Orientamenti" Costituzionali*, in *Osservatoriosullefonti.it*, n. 3/2023, 89-121.

ID., *The European path towards data quality and its standardisation in AI: a legal perspective*, in *BioLaw Journal – Rivista di BioDiritto*, n. 4/2022, 473-502.

MALASCHINI A, *Regolare l'intelligenza artificiale. Le risposte di Cina, Stati Uniti, Unione europea, Regno Unito, Russia e Italia*, in SEVERINO P. (*a cura di*), *Intelligenza artificiale, Politica, economia, diritto, tecnologia*, Roma, Luiss University Press, 2021, 104-169.

MARTIRE D., *Intelligenza artificiale e Stato costituzionale*, in *Diritto pubblico*, n. 2/2022, 397-444.

METCALF K.N., *e-Governance and Good Administration: Examples from Estonia*, in *European Review of Digital Administration & Law - ERDAL*, Volume 3, Issue 1, 2022, 73-82.

MOBILIO G., *La Corte EDU condanna il ricorso alle tecnologie di riconoscimento facciale per reprimere il dissenso politico – Osservazioni a partire dal caso Glukhin c. Russia*, in *DPCE online*, n. 1/2024, 695-705.

NAPOLITANO A., *Riflessioni sul ruolo del principio di precauzione nel processo decisionale delle pubbliche amministrazioni*, in *Diritto Pubblico Europeo Rassegna online*, n. 1/2019, 203-225.

NEUWIRTH R.J., *Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA)*, in *Computer Law & Security Review*, Volume 48, April 2023, 14.

NOVELLI C., *L'Artificial Intelligence Act Europeo: alcune questioni di implementazione*, in *federalismi.it*, n. 2/2024, 95-113.

NOVELLI C., CASOLARI F., ROTOLO A., TADDEO M., FLORIDI L., *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, v. 3, n. 13/2024.

OECD, *Recommendation of the Council on Artificial Intelligence*, 22.05.2019.

PARACAMPO M.T., *Il percorso evolutivo ed espansivo delle regulatory sandboxes da FinTech ai nuovi lidi operativi del prossimo futuro*, in *federalismi.it*, n. 18/2022, 207-232.

PINELLI C., *Disinformazione, comunità virtuali e democrazia: un inquadramento costituzionale*, in *Diritto Pubblico*, n. 1/2022, 173-197.

POUGET H. e ZUHDI R., *AI and Product Safety Standards Under the EU AI Act*, in *CarnegieEndowment.org*, il 5.03.2024.

POULLET Y., *Towards a New EU Regulatory Approach of the Digital Society*, in *European Review of Digital Administration & Law - ERDAL*, Volume 3, Issue 1, 2022, 113-124.

PWC: *Sizing the prize PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution What's the real value of AI for your business and how can you capitalise?.*

RESTA G., *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del Diritto*, n. 2/2019, 199-236.

ROBERTS H., COWLS J., HINE E., MORLEY J., WANG V., TADDEO M. & FLORIDI L., *Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes*, in *The Information Society*, 28/09/2022, 20.

SCHEPISI C., *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in FALCE V. (*a cura di*), *Strategia del dati e intelligenza artificiale – Verso un nuovo ordine giuridico del mercato*, Torino, G. Giappicheli Editore, 2023, 316, 53-75.

SIMONCINI A., *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, 63-89.

TOGNATO F., *Primo provvedimento del Tribunale in materia di DMA: i giudici di Lussemburgo respingono la domanda di sospensione proposta da Bytedance*, in *Eurojus.it*, il 4.03.2024.

TORREGIANI S., *La disciplina europea dei dati: dalla protezione alla governance*, Tesi di dottorato 2022, Università degli studi di Macerata, 317.

ID., *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in *Rivista italiana di informatica e diritto*, 2021, 47-65.

ID., *L'impatto dei dati non personali sulle decisioni algoritmiche: la prospettiva delle autorità amministrative indipendenti europee*, in *Osservatorio sulle fonti*, n. 2/2021, 807-829.

VEALE M. and BORGESIUS ZUIDERVEEN F., *Demystifying the Draft EU Artificial Intelligence Act!*, in *Computer Law Review International*, n. 4/2021, 97-112.

VON DER LEYEN U., *Un'Unione più ambiziosa – Il mio programma per l'Europa, orientamenti politici per la prossima Commissione europea 2019-2024*, 16 luglio 2019, pp. 14-15.

WULF A. J. and SEIZOV O., *Artificial Intelligence and Transparency: A Blueprint for Improving the Regulation of AI Applications in the EU*, in *European Business Law Review* 31, n. 4/2020, 611-640.

YORDANKA I., *The Data Protection Impact Assessment as a Tool to Enforce Non-Discriminatory AI*, disponibile in SSRN, in *Springer Proceedings of the Annual Privacy Forum* (Lisbon, 2020), 20.

ZENNER K., HACKER P. and HALLENSLEBEN S., *A vision for the AI Office: Rethinking digital governance in the EU*, in *Euractive*, il 23 maggio 2024.

ZUDDAS P., *Pregiudizi digitali e principio di precauzione*, in *Consulta online*, n. 2/2020, 408-425.