RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0125 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Stefano Torregiani

Il *Data Act*: una versione europea del *Data Nationalism*?

La datificazione ha contribuito alla silente e graduale erosione della sovranità dell'Unione europea: dalla miniera d'oro di dati prodotti dai cittadini europei hanno attinto sistematicamente soggetti stranieri, pubblici e privati, dotati di infrastrutture, tecnologie e competenze proprie, mentre gli Stati membri sono per lo più rimasti inerti e il tessuto industriale europeo è rimasto al palo del progresso digitale. Le ultime iniziative intraprese dal legislatore continentale in materia di "diritto dei dati" mirano ad arginare questa progressiva corrosione della autorità dell'Unione attraverso il rafforzamento di una impalcatura ordinamentale dimostratasi fin troppo vulnerabile. Questo contributo si focalizza sull'ultimo di tali provvedimenti normativi: il *Data Act*, ossia il testo regolamentare, di recente approvazione, volto a garantire una migliore allocazione del valore delle informazioni generate o raccolte nel contesto dell'utilizzo di prodotti e servizi appartenenti alle tecnologie dell'informazione e della comunicazione: ci si domanda se il sistema di circolazione dei dati immaginato dal legislatore dell'Unione è inquadrabile nel fenomeno del cd. *Data Nationalism* e se tale provvedimento potrà tradursi in un fruttuoso tentativo di difendere la sovranità europea attualmente in pericolo, se non proprio compromessa.

Regolamento sui dati – Localizzazione dei dati – Sovranità digitale – Diritto dei dati

Data Act: a European version of Data Nationalism?

The Datafication of the society led to the progressive decrease of the EU sovereignty: data produced by European citizens and companies have been systematically exploited by better equipped and skilled foreign players, thus holding European industrial and technological development back. Some of the acts lately enacted in the EU aim to overturn this detrimental situation through the update of the flawed European data law. This paper focuses on the last of the European Regulation concerning data law, i.e. the Data Act, through which EU institutions seek to reallocate the value of data produced or processed by means of information and communication technologies. Notably, it is questionable whether the data flow legislation setup in EU can be deemed as a Data Nationalism policy and whether this act could be a profitable attempt to defend the European sovereignty.

Data Act – Data Nationalism – Digital sovereignty – Data law

L'Autore è assegnista di ricerca presso l'Università degli Studi di Macerata

Questo contributo fa parte della sezione monografica *La fine di Internet? Vulnerabilità della democrazia e sfide della regolazione e gestione dello spazio digitale*, a cura di Simone Calzolaio con la collaborazione di Federico Serini

Sommario:. 1. Introduzione: l'Unione europea alla prova della datificazione. – 2. La regolazione della tecnologia: una questione di sovranità digitale. – 3. Il *Data Nationalism* e la tutela della sovranità. – 4. Il *Data Act* tra sovranità digitale, accesso e circolazione dei dati. – 5. Considerazioni conclusive: tra prospettive di sviluppo e rischio di isolazionismo.

1. Introduzione: l'Unione europea alla prova della datificazione

Il processo di datificazione delle realtà, ossia la trasformazione delle interazioni sociali in dati digitali quantificabili[1], ha portato alla configurazione di uno scenario globale in cui le informazioni, specie di carattere digitale, sono divenute una risorsa imprescindibile per la conduzione di qualsiasi attività di interesse sia pubblico sia privato[2]. In tale rinnovato contesto, i tradizionali elementi su cui si è storicamente basato il potere degli Stati sovrani sono stati messi fortemente in crisi dall'entrata in scena di nuovi attori che, tramite il controllo delle tecnologie su cui transitano i dati, hanno progressivamente acquisito la capacità di influenzare profondamente ogni aspetto della società nella quale viviamo.

Dal canto proprio, l'Unione europea ha dimostrato di patire enormemente tale congiuntura storica per una serie di ragioni di ordine tecnico e giuridico.

In primo luogo, la carenza di infrastrutture, di *expertise* e di investimenti paragonabili a quelli degli altri Stati rivali ha reso il vecchio continente un terreno piuttosto sterile per la crescita di operatori economici autoctoni in grado di sviluppare sistemi che possano quantomeno duellare con i vari GAFAM (Google, Apple, Facebook, Amazon, Microsoft) e BATX (Baidu, Alibaba, Tencent, Xiaomi)[3].

Tale "peccato originale" ha inevitabilmente aperto la strada allo sviluppo di una pesante dipendenza dai fornitori esteri, per la maggioranza siti in territorio statunitense, per la fruizione di servizi di natura latamente digitale (intelligenza artificiale, *cloud computing*, tecnologie 5G e similari)[4].

In secondo luogo, la tradizione costituzionale da cui provengono la maggior parte degli Stati membri dell'Unione europea – e da cui lo stesso ordinamento giuridico dell'Unione trae origine – non può che dimostrarsi refrattaria innanzi alla diffusione di un potere, quello delle *big tech*, che, per un verso, è in grado di influenzare la vita dei consociati in misura pari se non superiore a quella di una autorità pubblica democraticamente eletta, ma per un altro, difetta di qualsivoglia legittimazione popolare e non risulta pienamente conforme ai principi dello Stato di diritto[5].

Stanti le carenze sistemiche che affliggono il nostro continente e il rischio di erosione della

1. VanDijck 2014; Martoni 2020.
2. Surblyte 2016.
3. Polito 2021.
4. Già nel 2019 Kalff-Renda 2019, a p. 173, affermavano che: «current figures show that the bulk of Western world data (an estimated 92%) is currently stored in the United States, whereas only 4% is currently stored in Europe».
5. Non essendo infatti sufficienti i deludenti tentativi di vestire le piattaforme digitali di una parvenza di neutralità nei casi di insorgenza di controversie nascenti nel mondo online, come nell'ipotesi del *Facebook Oversight Board*; si veda in proposito Buratti 2022.

sovranità statuale che ne consegue, l'Unione europea ha reagito a tale situazione sfavorevole muovendosi, innanzitutto, verso la protezione dell'asset più prezioso a sua disposizione: i dati generati dai cittadini e dalle imprese nell'Unione europea. A tal fine, oltre al riconoscimento del diritto alla protezione dei dati personali[6], le istituzioni hanno di recente avviato una profonda riforma dell'ordinamento giuridico in materia di dati. In particolare, con la *Strategia europea per i dati* pubblicata nel 2020 la Commissione europea ha programmato le misure politiche e gli investimenti a sostegno dell'economia dei dati che le istituzioni e gli Stati membri avrebbero dovuto attuare nei successivi cinque anni al dichiarato scopo di rafforzare la sovranità dell'Unione[7].

Questo lavoro intende focalizzarsi su uno degli obiettivi prefigurati nella *Strategia*: la recente approvazione del Regolamento (UE) 2023/2854, noto anche con il nome di Data Act[8]. Nello specifico, verranno esaminati quegli elementi presenti nel testo del provvedimento normativo in questione che risultano utili a fornire una possibile risposta alla domanda che ha ispirato il titolo di questo contributo; si cercherà dunque di comprendere se questo (ennesimo) intervento del legislatore europeo si traduce in una chiusura delle frontiere digitali dell'Unione e, soprattutto, se un simile atteggiamento è in grado di garantire il raggiungimento degli obiettivi prefissati nella *Strategia europea per i dati*.

I paragrafi che seguono saranno dedicati, in primo luogo, alla perimetrazione del concetto di sovranità secondo il significato nuovo che esso ha assunto nell'epoca della datificazione. Successivamente, si passerà all'analisi del legame tra detto concetto e la regolazione della circolazione dei dati, prestando particolare attenzione all'atteggiamento di chiusura diffusosi negli ultimi anni negli ordinamenti giuridici di tutto il mondo. Da ultimo, si procederà ad una prima disamina di quei passaggi presenti nel *Data Act* che possono costituire una idonea base di partenza per comprendere l'orientamento politico del legislatore dell'Unione europea.

2. La regolazione della tecnologia: una questione di sovranità digitale

La corretta individuazione del significato che ha assunto il termine "sovranità" nell'attuale epoca digitale rappresenta una operazione tutt'altro che agevole.

La dottrina ha infatti rilevato l'esistenza di una pluralità di significati astrattamente riconducibili alla nozione di sovranità, la cui portata può assumere una accezione diversa a seconda del punto di vista dell'osservatore, sia esso di carattere giuridico, linguistico, politologico oppure sociale[9]. Qualunque sia il modo in cui la si vuole inquadrare, il comune denominatore di questo ventaglio di significati risiede in quel particolare potere riconosciuto a una organizzazione, storicamente di carattere politico, di esercitare la propria autorità all'interno di un territorio circoscritto, senza subire interferenze provenienti dall'esterno[10].

Adottando una prospettiva costituzionalistica, la sovranità costituisce l'elemento saliente del potere della autorità pubblica che, quantomeno a

6. Per la ricostruzione del percorso storico che ha portato al riconoscimento di tale diritto, si veda Gonzalez Fuster 2014.
7. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Una strategia europea per i dati", COM(2020) 66. In particolare, a pag. 6 la Commissione sottolinea che: «Il funzionamento dello spazio europeo di dati dipenderà dalla capacità dell'UE di investire nelle tecnologie e nelle infrastrutture di prossima generazione, come pure nelle competenze digitali, ad esempio l'alfabetizzazione ai dati (data literacy). Ciò contribuirà a sua volta a rafforzare la sovranità tecnologica dell'Europa per quanto riguarda le tecnologie e le infrastrutture abilitanti fondamentali per l'economia dei dati».
8. L'iter per l'entrata in vigore del provvedimento, iniziato il 23 febbraio 2022 con la pubblicazione della "Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo", denominato *Data Act*, è di recente giunto al termine giacché, dopo la sottoscrizione finale avvenuta in data 13 dicembre 2023, il provvedimento è stato pubblicato sulla Gazzetta ufficiale dell'Unione europea il 22 dicembre 2023.
9. Per un approfondimento, si veda Couture-Toupin 2019.
10. Pohle-Thiel 2020.

partire dal XVIII secolo, trova nel diritto tanto il suo fondamento, quanto la sua limitazione[11]. Se nella dimensione reale il potere sovrano da limitare era sempre stato quello riconosciuto al monarca o allo Stato-Ente, l'avvento della rivoluzione cibernetica ha sconvolto tale ordine[12], in quanto, introducendo una nuova dimensione nella nostra esistenza, quella virtuale, che si affianca e che impatta pesantemente su quella reale, ha ammesso nella corsa verso la sovranità attori nuovi, che mai prima d'ora avevano potuto vantare un potere equiparabile a quello di uno Stato sovrano.

In tale prospettiva, il processo di datificazione della realtà ha inesorabilmente spinto verso una riconsiderazione della definizione del concetto di "sovranità", non solo per quanto concerne la natura dei soggetti che possono effettivamente qualificarsi come titolari di sovranità, ma soprattutto per quanto riguarda le modalità attraverso le quali la sovranità stessa può essere esercitata. La questione non può più ridursi esclusivamente all'analisi del profilo soggettivo del detentore del potere (sovrano assoluto, entità statuale, popolo e così via), poiché oggi, forse come mai prima nella storia, assume una valenza tanto nuova quanto determinante il mezzo tecnico di cui il sovrano si avvale per acquisire e utilizzare il suo potere.

I commentatori più avveduti hanno individuato la caratteristica distintiva della sovranità dell'era digitale nel potere di calcolo e di automazione garantito dalla moderna tecnologia che, permettendo di prescindere in parte dall'azione umana, rende difficilmente controllabile e giustiziabile l'esercizio della autorità sovrana utilizzando i tradizionali canoni della normazione giuridica e del controllo pubblico[13].

La conseguenza inevitabile di tale cambio di paradigma, che segna altresì la differenza fondamentale tra sovranità e sovranità digitale, coincide con il notevole decremento di rilevanza dell'elemento della territorialità. Se prima il concetto rispecchiava il potere che l'organizzazione era in grado di esercitare su una territorialità definita e sui soggetti che su tale territorio transitavano[14], con l'avvento della rete Internet, caratterizzata per l'appunto dalla cosiddetta "a-territorialità"[15], la partita della sovranità non si gioca più solamente sul piano fisico-spaziale, ma anche su quello virtuale[16].

Ed è proprio su tale piano che le tradizionali entità statali, specie europee, fanno fatica ad imporsi: la sovranità nell'era digitale non può più prescindere dal mezzo tecnico[17], proprio perché attraverso di esso – e, come si vedrà, attraverso i dati che ne costituiscono la linfa vitale[18] – il potere sovrano viene esercitato: se una parte consistente della vita dei singoli si svolge in un ambiente cui è possibile accedere solamente tramite una infrastruttura – che dunque funge da portale interposto tra il reale e il virtuale – il controllo e la gestione

11. Simoncini 2017.
12. Simoncini 2019.
13. Simoncini 2017.
14. Pohle-Thiel 2020.
15. Gardini 2021, spec. pp. 296-301. Ma si veda sul punto Zeno-Zencovich 2016, spec. pp. 14-15, secondo cui l'idea della a-territorialità di Internet è stata oggi superata dalla progressiva espansione dell'intervento statale nella regolazione delle reti.
16. Eloquenti in proposito le parole rilasciate nel 2020 dall'allora presidente del Garante per la protezione dei dati personali italiano, Antonello Soro, il quale ha affermato che: «In uno spazio "defisicizzato" come la rete la sovranità va declinata in forme nuove, meno legate al tradizionale criterio di territorialità e più attente, invece, alla capacità degli Stati di rendere effettiva la tutela dei diritti e la stessa forma democratica, di fronte a sempre nuove spinte illiberali. Sono significativi, in tal senso, i rischi cui un uso manipolativo dei dati personali, anche da parte di potenze estere, può avere sulla sovranità nazionale e sulle scelte politiche essenziali che ne determinano l'esercizio», intervista ad Antonello Soro, aprile 2020, in sito GPDP (doc-web 9317569).
17. Come è stato correttamente puntualizzato da Simoncini 2017: «La sovranità, infatti, oggi non ha più caratteri necessariamente privati o pubblici, personali o collettivi, ma essenzialmente tecnici».
18. Polatin-Reuben-Wright 2014 si riferiscono direttamente al sintagma "data sovereignty" definendolo «the attempt by nation-states to subject data flows to national jurisdictions».

di quella infrastruttura porta con sé l'automatica acquisizione di una autorità sostanzialmente parificabile al potere sovrano che uno Stato vanta sul proprio territorio[19].

Questa svolta epocale ha pesantemente scosso le fondamenta delle democrazie occidentali, le quali si sono trovate costrette a concorrere non più solamente con altre entità pubbliche statuali – come avveniva nell'epoca della sovranità "pre-digitale" – ma con soggetti di natura privata che, proprio grazie al controllo degli strumenti tecnologici, possono esercitare una influenza su un determinato territorio senza neanche la necessità di entrarvi[20].

Dalla presa di coscienza di questa nuova situazione di fatto nascono le più recenti iniziative europee di "regolazione della tecnologia", le quali, benché in linea con quanto avvenuto a partire dagli anni Novanta con la diffusione di Internet[21], si sono moltiplicate negli anni più recenti. Non a caso una delle prime volte in cui il termine trova spazio nelle dichiarazioni ufficiali di esponenti dei governi degli Stati membri coincide con la presentazione dell'iniziativa di Germania e Francia finalizzata alla realizzazione di una infrastruttura digitale di matrice europea, il celebre progetto GAIA-X[22]. Essendo lo scopo quello di predisporre un'alternativa alle big tech estere per la conservazione dei dati dei cittadini e delle imprese europee[23], appare evidente come la realizzazione di siffatto progetto abbia plasmato pesantemente la nozione di sovranità digitale che ha ispirato le azioni delle istituzioni europee[24].

3. Il *Data Nationalism* e la tutela della sovranità

Di fronte all'ingresso delle società private nella contesa verso quella sovranità che prima spettava solo agli Stati, molte entità pubbliche, nazionali o sovranazionali, hanno risposto con l'adozione di numerosi atti normativi, nel tentativo di tamponare il rapido processo di erosione del loro potere. In tale ottica, ognuno dei provvedimenti legislativi aventi ad oggetto la regolazione di una delle svariate dimensioni del mondo della tecnologia digitale vanta infatti una connessione, diretta o indiretta, con il concetto di sovranità. Basti pensare, con riguardo allo scenario europeo, al cosiddetto diritto dei dati (o *data law*)[25], alla proposta di regolazione dell'intelligenza artificiale[26], al *Digital Market Act* o al *Digital Services Act*[27].

19. VanDijck 2020.
20. Cremona 2021.
21. Bertola 2022. Come riconosce l'A., i tentativi di regolazione della rete emersi a cavallo del nuovo millennio si sono caratterizzati più per il modello del "multistakeholderismo", dove governi e teorici della rete libera decidevano di riconoscersi reciproche concessioni in materia di normazione di Internet, piuttosto che per un sistema di regolazione maggiormente prescrittivo tipico della *hard law*.
22. Santaniello 2022.
23. Pagnanelli 2021.
24. È bene notare che il concetto di sovranità varia enormemente a seconda del contesto giuridico e politico di riferimento. In tal senso, la sovranità digitale europea non corrisponderà alla differente declinazione che la nozione di sovranità assume, ad esempio, nella Repubblica popolare cinese, su cui, per un approfondimento si rimanda a Creemers 2020.
25. Con questa espressione si suole fare riferimento a tutte le normative aventi ad oggetto i "dati" generalmente intesi e non solamente a quelle in materia di protezione dei dati personali. Per un approfondimento si veda Streinz 2021.
26. La Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione, 21 aprile 2021, COM(2021) 206, più volte modificata, non è ancora entrata in vigore in quanto non risulta ancora concluso l'iter di approvazione.
27. Ci si riferisce, rispettivamente, al 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) e al Regolamento (UE) 2022/2065 del

Fra la vasta gamma di fonti legislative che possono assumere rilievo in tale contesto, il presente lavoro si focalizza sul *data law*: attesa la funzione essenziale e prodromica che la tecnica di trasmissione dei dati ricopre rispetto a tutte le tecnologie digitali oggi disponibili, la regolazione di dette tecnologie deve necessariamente passare attraverso la regolazione della gestione e della circolazione dei dati che le alimentano[28].

Non risulta allora affatto sorprendente che una delle reazioni al fenomeno della datificazione statisticamente più diffuse tra i legislatori di tutti i Paesi del mondo sia stata proprio quella di varare misure normative di *data localization*, consistenti nell'adozione di prescrizioni normative o prassi amministrative che impongono, direttamente o indirettamente, il luogo in cui deve essere effettuato un determinato trattamento oppure che fissano le condizioni per il trasferimento dei dati al di fuori dei confini nazionali[29].

Questa ventata di protezionismo digitale non ha interessato solamente gli Stati membri dell'Unione europea[30], storicamente più sensibile alle questioni di protezione dei dati, specialmente personali, ma ha parimenti riguardato altri Paesi che, intimoriti dall'enorme potere guadagnato dalle *big tech* e dalle nazioni tecnologicamente più avanzate, hanno ritenuto opportuno chiudere le proprie frontiere digitali[31].

È proprio in tale contesto che si avverte in maniera compiuta il passaggio dalla "digital sovereignty" alla "data sovereignty", intesa come «spectrum of approaches adopted by different states to control data generated in or passing through national internet infrastructure»[32], dove tale seconda categoria costituisce un sottoinsieme della prima[33].

Pertanto, l'introduzione di obblighi di localizzazione dei dati viene generalmente interpretata dai legislatori come una delle possibili vie – forse la più percorsa vista l'apparente immediatezza del risultato che è in grado di garantire – per proteggere o riprendere la propria sovranità[34].

Tale ordine di idee ha portato negli ultimi decenni al consolidamento di un fenomeno che è stato dalla dottrina definito come "Data Nationalism"[35]. Detta espressione descrive il novero di politiche che si sono diffuse a partire dalla rivelazione dei programmi di sorveglianza di massa implementati dagli Stati Uniti e che hanno portato all'incremento esponenziale delle misure di localizzazione dei dati[36].

Gli studiosi che si sono occupati delle questioni di *Data Nationalism* e di obblighi di localizzazione non hanno dubbi in merito al fatto che l'attuazione di tali politiche sia più deleteria che vantaggiosa per i singoli governi, giacché la frammentazione di uno spazio ontologicamente interconnesso e senza confini come la rete Internet non farebbe altro che frenare l'innovazione e pregiudicare lo sviluppo delle economie domestiche[37].

Al contempo, non ci si può tuttavia esimere dal constatare che la realtà dei fatti ha, a volte, dimostrato che la sede principale dell'operatore economico che fornisce un qualsiasi servizio nel settore ICT e, conseguentemente, la sede in cui i dati vengono conservati hanno una importanza dirimente per gli equilibri geopolitici. Stati Uniti e Cina su tutte ne costituiscono un esempio lampante: il fatto che i più grandi operatori privati OTT siano nati

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).

28. DellaMorte 2018, p. 135; Aktoudianakis 2020, p. 3.
29. Ferracane 2017, spec. pp. 2-3.
30. Ryan-Falvey-Merchant 2013.
31. Ad esempio, Savelyev 2016 tratta il caso della Russia.
32. Polatin-Reuben-Wright 2014.
33. Boncinelli 2021, spec. p. 41.
34. Ferracane 2017, spec. p. 6.
35. Chander-Lê 2015; Castro 2013.
36. Chander-Lê 2015.
37. Bauer-LeeMakiyama-Van der Marel-Verschelde 2014; Chander-Lê 2015, spec. pp. 713-739; Castro 2013.

e abbiano la sede principale in detti Paesi fa sì che i rispettivi governi siano in una posizione di gran lunga più favorevole per beneficiare – di riflesso o per imposizione normativa – del potere garantito dal controllo del mezzo tecnico.

Quanto agli Stati Uniti, sono numerosi gli episodi che testimoniano la fondatezza di tale assunto. Si pensi alla nota prassi diffusa fra le autorità pubbliche di chiedere accesso alle informazioni detenute da imprese private[38]; all'ormai celeberrimo caso *Datagate* relativo alle rivelazioni dell'ex dipendente della CIA, Edward Snowden, concernenti il programma di sorveglianza di massa attuato dagli Stati Uniti[39]; o, da ultimo, all'entrata in vigore nel 2018 del *Clarifying Lawful Overseas Use of Data Act*, noto come *Cloud Act*, il quale impone agli *electronic communications services providers* e ai *remote computing service providers* di consentire alle sole autorità americane l'accesso ai dati relativi agli utenti indipendentemente dal luogo in cui tali informazioni sono localizzate[40].

Parimenti, l'ordinamento giuridico della Repubblica popolare cinese, oltre a consentire alla pubblica autorità l'accesso alle informazioni nella disponibilità di soggetti privati[41], ha coniato i concetti di *important data* e di *national core data* al fine di assicurare un maggiore controllo pubblico su informazioni che vantano uno stretto legame con la sicurezza nazionale, lo sviluppo economico e gli interessi del Paese[42].

Innanzi al progressivo consolidamento di tale quadro fattuale, caratterizzato da una accesa frizione tra diritto e tecnologia e da una progressiva concentrazione di potere in capo a entità pubbliche e private localizzate all'infuori del territorio europeo, l'Unione europea ha intrapreso un lento cammino di riforme volto a rielaborare l'architettura dell'ordinamento continentale in materia di protezione e circolazione dei dati personali e non personali[43].

Tale percorso, ancora *in itinere*, ha di recente raggiunto due traguardi di estrema rilevanza, i quali rappresentano, in un certo senso, una prima e rilevante risposta del legislatore innanzi ai mutamenti economico-sociali di cui si è detto. Si tratta, da un lato, del *Data Governance Act*[44], e, dall'altro, dal *Data Act*[45].

Il paragrafo che segue si concentrerà sul secondo di questi atti normativi allo scopo di comprendere se la nuova direzione intrapresa dal legislatore eurounitario si inserisce nel solco di quelle iniziative riconducibili alle politiche di *Data Nationalism* come sopra delineate.

4. Il *Data Act* tra sovranità digitale, accesso e circolazione dei dati

Per trovare una risposta al quesito che ha stimolato la redazione del presente scritto occorre svolgere una breve premessa utile a comprendere se la volontà del legislatore europeo sia effettivamente quella di promuovere una politica di protezionismo delle proprie informazioni, limitando (ulteriormente) la circolazione dei dati al di fuori del territorio continentale.

38. Cate-Kuner-Millard-Svantesson 2014. Anche se non mancano casi di operatori che si sono opposti a tale prassi, si vedano al riguardo Rubechi 2016, spec. p. 23; Orofino 2016.
39. Nino 2013.
40. Cantekin 2018; Christakis-Terpan 2021.
41. Wang 2012.
42. Pagnanelli 2021, spec. pp. 20-21.
43. Per una puntuale ricostruzione della evoluzione della disciplina in materia di protezione dei dati personali, si veda Calzolaio 2017; per una disamina della disciplina europea in materia di dati non personali, sia consentito rinviare a Torregiani 2020.
44. Si tratta del 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*).
45. 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*).

L'approvazione del Regolamento (UE) 2016/679 prima[46], e del Regolamento (UE) 2018/1807 poi[47], hanno plasmato un diritto dei dati europeo dicotomico in quanto costruito sulla distinzione tra i dati a carattere personale, ossia quelli riguardanti una persona fisica identificata o identificabile[48], e quelli non personali, che invece includono tutte le informazioni non rientranti nella prima categoria[49].

Il quadro normativo che ne è derivato si caratterizza per un evidente squilibrio tra le due categorie di dati, giacché, se da un lato i dati a carattere personale sono oggetto di una articolata e capillare regolazione, dall'altro, la fattispecie dei dati non personali non ha ricevuto, quantomeno nel 2018, pari attenzione da parte delle istituzioni europee.

Tale sviluppo si è tradotto in un profondo divario anche con riguardo ai due corrispondenti regimi di circolazione dei dati: se i dati personali possono uscire dai confini europei solo nel rispetto delle stringenti condizioni previste dal capo V del GDPR[50], per quelli non personali il Regolamento (UE) 2018/1807 ha cercato di liberalizzare la circolazione all'interno dei confini continentali, ma ha totalmente tralasciato la dimensione relativa alla circolazione esterna di queste informazioni[51].

L'assetto ordinamentale così formatosi è sin da subito parso troppo distante dalla realtà fattuale del mondo digitalizzato, sia perché prescinde dalle difficoltà di procedere a una esatta distinzione fra dati personali e non[52], sia perché sottovaluta colpevolmente l'impatto che il trattamento dei dati a carattere non personale può avere sulla società e sulla sovranità dell'Unione[53].

Queste, in estrema sintesi, sono le premesse dalle quali muove il *Data Act*[54]: il testo del provvedimento rappresenta un interessante indicatore della presa di coscienza da parte dell'Unione delle carenze del proprio impianto ordinamentale e dei mutamenti che investiranno il diritto europeo dei dati negli anni a venire.

In proposito, il *Data Act* e l'altro regolamento recentemente approvato, il *Data Governance Act*, costituiscono provvedimenti normativi tra loro comunicanti e il cui scopo ultimo risiede nella creazione di un nuovo modello "europeo" di governance dei dati quale strumento utile, da un lato, a rallentare l'accumulo esponenziale di potere in capo ai soggetti, pubblici e privati, esterni all'Unione e, dall'altro, a proteggere la sovranità degli Stati membri anche attraverso la riduzione della quantità dei dati che, fuoriuscendo dal territorio europeo,

46. Si tratta del 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 o, dall'acronimo inglese, GDPR).
47. Si tratta del Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.
48. Così recita l'art. 4, punto 1) del GDPR.
49. L'art. 3, punto 1) del Regolamento (UE) 2018/1807 li definisce come «i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679».
50. Nello specifico, gli articoli dal 44 al 50 del GDPR prevedono come condizione per il trasferimento dei dati al di fuori dell'Unione europea, una tra le seguenti: una decisione di adeguatezza della Commissione europea; la predisposizione di garanzie adeguate; il ricorso a norme vincolanti d'impresa; un accordo internazionale per le decisioni di autorità estere; la sussistenza di una delle deroghe previste dall'art. 49 del GDPR.
51. Per una trattazione più approfondita, sia consentito rinviare a Torregiani 2021.
52. Montagnani 2019, pp. 311-313.
53. Per un approfondimento sia consentito rinviare a Torregiani 2021a.
54. Tra l'altro, è lo stesso testo del *Data Act* a rimarcare la necessità di integrare il Regolamento sui dati non personali, anche se con specifico riferimento al tema dei codici di condotta di autoregolamentazione per agevolare il passaggio a un diverso fornitore di servizi di trattamento dei dati e per la portabilità dei dati. In proposito, l'art. 1 par. 7 prevede espressamente che: «Il presente regolamento integra l'approccio di autoregolamentazione di cui al regolamento (UE) 2018/1807 aggiungendo obblighi di applicazione generale relativi al passaggio ad altri servizi cloud».

sono destinati a divenire una risorsa preziosa per un'autorità o un'industria extraeuropea.

A tal fine, il *Data Act* si pone in perfetta continuità con il *Data Governance Act*, giacché, a fronte di un obiettivo che può dirsi per certi versi unitario[55], dedica le sue prescrizioni ad ambiti in parte diversi rispetto al Regolamento (UE) 2022/868[56], nel tentativo di completare il disegno globale in materia di gestione dei dati generati in territorio europeo. In particolare, il *Data Act* inserisce una nuova gamma di diritti e di corrispondenti doveri al fine di agevolare l'accesso ai dati da parte dei soggetti più deboli del ciclo di raccolta e trattamento dei dati e da parte di enti pubblici che potrebbero necessitare delle informazioni detenute dai privati in particolari situazioni emergenziali. Conseguentemente, il Regolamento detta le condizioni e le modalità affinché i dati detenuti da chi fabbrica prodotti o offre servizi capaci di raccogliere e trattare informazioni siano messi a disposizione dell'utente o, su richiesta di quest'ultimo, di fornitori di servizi terzi, prescrivendo per diversi attori dell'attuale panorama dell'economia digitale nuove disposizioni in materia di trasferimento dei dati, validità delle clausole contrattuali e interoperabilità[57].

In sostanza, la sua funzione primaria appare essenzialmente quella di garantire una migliore allocazione del valore delle informazioni tra i differenti attori che intervengono nelle *value chains* dell'economia dei dati[58], avuto particolare riguardo ai dati generati o raccolti nel contesto dell'utilizzo di prodotti e servizi rientranti nell'ambito dell'*Internet of Things* o di servizi *cloud* e di trattamento dei dati generalmente intesi[59].

55. La parte introduttiva della proposta originaria del *Data Act* afferma espressamente che «La presente proposta integra l'atto sulla governance dei dati adottato di recente». In proposito, si veda la Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), 23 febbraio 2022, COM(2022) 68, p. 5.
56. Il *Data Governance Act* si focalizza, in particolare sui seguenti quattro profili: a) il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici; b) un quadro di notifica e controllo per la fornitura di servizi di intermediazione dei dati; c) un quadro per la registrazione volontaria delle entità che raccolgono e trattano i dati messi a disposizione a fini altruistici; d) un quadro per l'istituzione di un comitato europeo per l'innovazione in materia di dati – comitato che, tra l'altro, viene richiamato anche dall'art. 42 del *Data Act*. Per un approfondimento in materia di *Data Governance Act*, si veda Iannuzzi 2021.
57. L'obiettivo del *Data Act* è sintetizzato dal considerando n. 5, il quale recita: «Il presente regolamento garantisce che gli utenti di un prodotto connesso o di un servizio correlato nell'Unione possano accedere tempestivamente ai dati generati dall'uso di tale prodotto connesso o servizio correlato e che tali utenti possano utilizzare i dati, anche condividendoli con terzi di loro scelta. Esso impone ai titolari dei dati l'obbligo di mettere i dati a disposizione degli utenti e dei terzi scelti dagli utenti in determinate circostanze. Garantisce inoltre che i titolari dei dati mettano i dati a disposizione dei destinatari dei dati nell'Unione a condizioni eque, ragionevoli e non discriminatori e in modo trasparente. Le norme di diritto privato sono fondamentali nel quadro generale della condivisione dei dati. Il presente regolamento adegua pertanto le norme di diritto contrattuale e impedisce lo sfruttamento degli squilibri contrattuali che ostacolano l'accesso equo ai dati e il loro utilizzo. Il presente regolamento garantisce inoltre che i titolari dei dati mettano a disposizione degli enti pubblici, della Commissione, della Banca centrale europea o degli organismi dell'Unione, ove vi sia una necessità eccezionale, i dati necessari per lo svolgimento di un compito specifico nell'interesse pubblico. Il presente regolamento mira altresì ad agevolare il passaggio tra servizi di trattamento dei dati e a migliorare l'interoperabilità dei dati e dei meccanismi e servizi di condivisione dei dati nell'Unione. È opportuno non interpretare il presente regolamento come un atto che riconosce o che conferisce ai titolari dei dati un nuovo diritto di utilizzare i dati generati dall'uso di un prodotto connesso o di un servizio correlato».
58. European Commission 2021.
59. L'art. 1, par. 1 del *Data Act*, individua come oggetto del Regolamento «tra l'altro: a) la messa a disposizione dei dati del prodotto connesso e di un servizio correlato all'utente del prodotto connesso o del servizio correlato; b) la messa a disposizione di dati da parte dei titolari dei dati ai destinatari dei dati; c) la messa a disposizione di dati da parte dei titolari dei dati agli enti pubblici, alla Commissione, alla Banca centrale europea e a organismi

Per quanto di interesse ai fini del presente contributo, il capo II è dedicato alla condivisione dei dati da impresa a consumatore e da impresa a impresa e contiene le modalità attraverso cui i produttori debbono consentire agli utenti dei prodotti e dei servizi correlati, o ai terzi dagli stessi indicati, l'accesso ai dati generati durante l'utilizzo del prodotto o del servizio[60]; il capo III individua gli obblighi di messa a disposizione delle informazioni per i titolari dei dati[61]; il capo IV disciplina le clausole contrattuali abusive dirette a limitare illegittimamente l'accesso ai dati per altre imprese; il capo V indica le condizioni al verificarsi delle quali sussiste l'obbligo di mettere i dati a disposizione di enti pubblici; il capo VI regola il passaggio da un fornitore di servizi di trattamento dei dati a un altro; con il capo VII viene disciplinato l'accesso e il trasferimento dei dati non personali; mentre il capo VIII introduce le prescrizioni relative alla interoperabilità.

Dall'esame delle disposizioni presenti nei capi citati, appare evidente che il *Data Act* è destinato, in primo luogo, a incidere sul tema della proprietà dei dati industriali, ossia sull'ipotizzato riconoscimento di un diritto di proprietà concernente il bene immateriale "dato". Storicamente, le correnti della dottrina economico-giuridica che si sono contrapposte su questo campo hanno visto, da un lato, i fautori dell'introduzione di una privativa vera e propria e, dall'altro, i sostenitori di un differente approccio basato esclusivamente sul riconoscimento di un diritto di accesso in favore dei soggetti intervenuti nel processo di generazione del dato[62].

Con l'approvazione del *Data Act*, le istituzioni europee sembrano aver optato in maniera decisa per la seconda di queste alternative: si riconosce al soggetto debole del rapporto contrattuale nascente dall'utilizzo delle tecnologie digitali – l'utente/consumatore – un diritto di accedere alle informazioni dallo stesso generate, sì da compensare lo squilibrio di potere negoziale patito nei confronti delle grandi compagnie produttrici o fornitrici dei servizi, le quali solitamente hanno la capacità tecnica di escludere gli altri dall'accesso ai dati raccolti[63].

Ad uno sguardo più attento, nelle disposizioni del nuovo Regolamento è inoltre possibile intravedere la volontà dell'Unione di difendersi dagli attacchi alla propria *data sovereignty* provenienti dall'esterno.

dell'Unione, a fronte di necessità eccezionali per tali dati, per l'esecuzione di un compito specifico svolto nell'interesse pubblico; d) la facilitazione del passaggio da un servizio di trattamento dei dati all'altro; e) l'introduzione di garanzie contro l'accesso illecito di terzi ai dati non personali; e f) lo sviluppo di norme di interoperabilità per i dati a cui accedere, da trasferire e utilizzare».

60. L'art. 2 del *Data Act* definisce al punto 6) il "servizio correlato" come «un servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto al momento dell'acquisto, della locazione o del noleggio in modo tale che la sua assenza impedirebbe al prodotto connesso di svolgere una o più delle sue funzioni o che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto connesso»; al punto 15) i "dati del prodotto" come i «dati generati dall'uso di un prodotto connesso e progettati dal fabbricante in modo tale che un utente, un titolare dei dati o un terzo, compreso se del caso il fabbricante, possano reperirli tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo»; e, al punto 16) i "dati di un servizio correlato" come i «dati che rappresentano la digitalizzazione delle azioni o degli eventi degli utenti relativi al prodotto connesso, registrati intenzionalmente dall'utente o generati come sottoprodotto dell'azione dell'utente durante la fornitura di un servizio correlato da parte del fornitore».
61. Il "titolare dei dati" viene definito dall'art. 2, punto 13) del *Data Act* come la «persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato».
62. Per un approfondimento si vedano Drexl 2016; Wiebe 2016.
63. Con riferimento alla cosiddetta escludibilità, ossia la possibilità di escludere gli altri dalla conoscenza di una determinata informazione tramite l'implementazione di misure tecniche *ad hoc* si veda Kerber 2016.

In primo luogo, il *Data Act* attribuisce agli utenti e alle imprese europee il diritto di ottenere l'accesso ad informazioni che altrimenti rimarrebbero nella esclusiva disponibilità delle grandi compagnie tecnologiche che, come detto, sono per la maggior parte locate al di fuori dei confini continentali[64]. Sotto tale profilo, il *Data Act* sembra porsi sul versante opposto rispetto a quegli atti normativi extra-europei, su tutti il *Cloud Act* statunitense[65], volti a consentire l'accesso a informazioni che potrebbero essere archiviate in server situati in territori rispondenti ad altre giurisdizioni[66].

In secondo luogo, la volontà del legislatore traspare in maniera ancor più evidente con riferimento all'obbligo per il titolare dei dati di mettere i dati in suo possesso a disposizione di terzi indicati dall'utente, come previsto dall'articolo 5 del *Data Act*. Il paragrafo terzo di tale disposizione esclude *expressis verbis* dal novero dei "terzi" riceventi quelli che vengono designati dalla Commissione europea come *gatekeepers*[67], i quali, ricoprendo la posizione di soggetti che dettano le condizioni per l'accesso al mercato[68], coincidono, in sostanza, con le *big tech* aventi sede in Paesi terzi[69]. In altri termini, in virtù di tale preclusione, i *gatekeepers* non possono vantare il medesimo diritto di ottenere i dati detenuti da altri operatori sulla base di una richiesta di trasferimento promossa dall'utente[70].

Dall'altro lato, invece, il *Data Act* concerne anche il versante relativo alla circolazione esterna dei dati non personali generati nel contesto

64. Eloquente in tal senso l'art. 1, par. 3 del *Data Act* che nel definire l'ambito di applicazione soggettivo del Regolamento stabilisce che: «Il presente regolamento si applica: a) ai fabbricanti di prodotti connessi immessi sul mercato dell'Unione e ai fornitori di servizi correlati, indipendentemente dal loro luogo di stabilimento di tali fabbricanti e fornitori; b) agli utenti nell'Unione di prodotti connessi o servizi correlati di cui alla lettera a); c) ai titolari dei dati, indipendentemente dal loro luogo di stabilimento, che mettono dati a disposizione dei destinatari dei dati nell'Unione; d) ai destinatari dei dati nell'Unione a disposizione dei quali sono messi i dati; e) agli enti pubblici, alla Commissione, alla Banca centrale europea e agli organismi dell'Unione che chiedono ai titolari dei dati di mettere i dati a disposizione nel caso tali dati siano necessari a fronte di una necessità eccezionale per l'esecuzione di un compito specifico svolto nell'interesse pubblico e ai titolari dei dati che forniscono tali dati in risposta a tale richiesta; f) ai fornitori di servizi di trattamento dei dati, indipendentemente dal loro luogo di stabilimento, che forniscono tali servizi a clienti nell'Unione; g) ai partecipanti agli spazi di dati, ai venditori di applicazioni che utilizzano contratti intelligenti e alle persone la cui attività commerciale, imprenditoriale o professionale comporti l'implementazione di contratti intelligenti per altri nel contesto dell'esecuzione di un accordo».
65. Cerrina Feroni 2022.
66. Per un approfondimento in merito alle problematiche giuridiche legate al fenomeno cloud si veda Boncinelli 2021.
67. L'art. 5, par. 3 del *Data Act* si riferisce a «Qualsiasi impresa designata come gatekeeper a norma dell'articolo 3 del regolamento (UE) 2022/1925», il quale, a sua volta, prevede l'attribuzione di tale qualifica per le imprese che a) hanno un impatto significativo sul mercato interno; b) forniscono un servizio di piattaforma di base che costituisce un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali; c) detengono una posizione consolidata e duratura, nell'ambito delle proprie attività, o è prevedibile che acquisiscano siffatta posizione nel prossimo futuro.
68. Contaldi 2021.
69. Gallese 2022.
70. Eloquente in tal senso il considerando n. 40 nella parte in cui afferma che «è emerso un piccolo numero di imprese molto grandi con un notevole potere economico nell'economia digitale, ottenuto grazie all'accumulo e all'aggregazione di grandi volumi di dati e all'infrastruttura tecnologica per la loro monetizzazione. Tali imprese molto grandi includono imprese che forniscono servizi di piattaforma di base che controllano interi ecosistemi di piattaforme nell'economia digitale e che gli operatori di mercato esistenti o nuovi non sono in grado di sfidare o contrastare. […] data la capacità inarrivabile di tali imprese di acquisire dati, l'inclusione dei gatekeeper quali beneficiari del diritto di accesso ai dati non è necessaria per conseguire l'obiettivo del presente regolamento, e sarebbe pertanto sproporzionata per i titolari dei dati soggetti a tali obblighi».

europeo, dunque quella dimensione colpevolmente rimasta senza disciplina nell'ambito del Regolamento (UE) 2018/1807.

L'articolo 32 del *Data Act* esordisce imponendo in capo ai fornitori di servizi di trattamento dei dati l'obbligo di adozione delle misure tecniche, organizzative e giuridiche necessarie a impedire l'accesso governativo internazionale di Paesi terzi ai dati non personali detenuti nell'Unione e il trasferimento di detti dati in tutte le ipotesi in cui tali operazioni dovessero contrastare con il diritto eurounitario o degli Stati membri[71].

Nel caso in cui il trasferimento sia richiesto da decisioni o sentenze di un organo giurisdizionale o di un'autorità amministrativa di un Paese terzo, i paragrafi successivi dell'articolo citato condizionano il trasferimento alla sussistenza di un accordo internazionale o, in assenza di questo, al rispetto di una serie di guarentigie fra le quali compaiono la motivazione e la proporzionalità della richiesta, l'esame dell'opposizione eventualmente sollevata dal soggetto richiesto e l'obbligo di tenere in considerazione gli interessi di quest'ultimo[72].

In tal senso, il *Data Act* ribadisce quanto già disposto dal *Data Governance Act* in materia di trasferimento di dati non personali, indirizzando disposizioni nella sostanza simili verso la particolare categoria dei fornitori di servizi di trattamento di dati[73].

Anche in quest'ottica, dunque, tanto il *Data Governance Act* quanto il *Data Act* costituiscono una chiara risposta del legislatore europeo alla entrata in vigore di atti normativi esteri capaci di ridurre la sovranità sui dati europei. Le preoccupazioni relative all'accesso illecito da parte delle amministrazioni pubbliche di Paesi terzi[74], hanno condotto a un cambiamento di impostazione consistente nella trasposizione dei principi e delle regole stabiliti dal capo V del GDPR, che già di per sé costituivano una misura di *data localization*, nel diverso ambito dei dati non personali.

Dalle norme testé esaminate emerge in maniera chiara la volontà delle istituzioni europee di procedere verso la creazione di un sistema che permetta all'Unione di mantenere un maggiore controllo sulle sorti dei dati generati in ambito continentale. Fra le righe del *Data Act* è possibile scorgere una accentuazione di quella tendenza alla localizzazione dei dati all'interno dell'Unione europea inaugurata con l'entrata in vigore del GDPR per le informazioni a carattere personale. Oltre al rinnovato rilievo assunto dalla categoria dei dati non personali in seno ai due regolamenti più recenti, le disposizioni in tema di accesso e di trasferimento consentono di collocare il *Data Act* all'interno del novero delle politiche normative riconducibili al fenomeno del *Data Nationalism*.

Con tale provvedimento, il legislatore punta infatti alla limitazione del potere di ingerenza esercitato dagli attori esterni al circuito eurounitario attraverso un duplice meccanismo di esclusione. Da un lato, viene varata una normativa che preclude espressamente i benefici del diritto di accesso per quei soggetti privati che, secondo la valutazione della Commissione europea, sono in grado di alterare gli equilibri di mercato e che, allo stato attuale, risiedono tutti negli Stati Uniti o nella

71. A norma dell'art. 2, punto 8) del *Data Act*, il "servizio di trattamento dei dati" consiste in un «un servizio digitale fornito a un cliente e che consente l'accesso di rete universale e su richiesta a un pool condiviso di risorse informatiche configurabili, scalabili ed elastiche di natura centralizzata, distribuita o altamente distribuita e che può essere rapidamente erogato e rilasciato con un minimo sforzo di gestione o interazione con il fornitore di servizi»; per una descrizione più dettagliata, si vedano i considerando 80 e 81. A titolo esemplificativo, si segnala che in tale categoria rientrano i servizi di servizi *cloud* ed *edge computing*.

72. Art. 32, parr. 2 e 3 del *Data Act*.

73. L'art. 31 del Regolamento (UE) 2022/868 (*Data Governance Act*) prescrive le medesime condizioni e obblighi per l'accesso e il trasferimento internazionale dei dati non personali quando coinvolge enti pubblici, titolari del diritto di riutilizzo dei dati, fornitori di servizi di intermediazione dei dati e organizzazioni per l'altruismo dei dati.

74. Già la Proposta di *Data Act* affermava nella parte introduttiva 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)», p. 3.

Repubblica popolare cinese[75]. Dall'altro lato, il *Data Act* ha introdotto ulteriori obblighi di localizzazione di dati con riguardo ad una categoria di informazioni che prima, salvo specifiche normative di settore, poteva liberamente lasciare il territorio dell'Unione, mentre ora – o meglio, quando il *Data Act* diverrà applicabile[76] – impedisce l'indiscriminato e massivo trasferimento internazionale di dati non personali.

5. Considerazioni conclusive: tra prospettive di sviluppo e rischio di isolazionismo

L'ingresso nell'era digitale ha scatenato una feroce competizione per il controllo dei dati poiché da tale controllo passa il mantenimento o l'acquisizione della sovranità degli Stati e delle organizzazioni internazionali. Se gli operatori privati agiscono muovendosi sul piano prettamente tecnico attraverso la realizzazione di infrastrutture e di sistemi tecnologici in grado di rendere sempre più profittevole il trattamento dei dati, le entità pubbliche hanno intrapreso una battaglia che si combatte soprattutto a colpi di atti normativi.

In questo senso, i recenti sviluppi dell'ordinamento europeo dei dati, culminati con l'entrata in vigore del *Data Act*, dimostrano che l'intenzione del legislatore europeo va al di là del semplice rafforzamento del mercato unico, come imporrebbe la base giuridica su cui vengono fondati quasi tutti i provvedimenti legislativi in materia[77]. Il *Data Act*, così come il *Data Governance Act*, sembrano infatti essere stati concepiti come strumenti utili anche alla realizzazione di un modello "europeo" di gestione dei dati, e delle tecnologie digitali in generale, la cui finalità ultima risiede nella difesa della sovranità continentale.

Pertanto, se, da una parte, il *Data Act* mira a incentivare la concorrenzialità e lo sviluppo di prodotti e servizi maggiormente innovativi aumentando la disponibilità e la condivisione dei dati all'interno dell'Unione, dall'altra parte, lo stesso provvedimento fa parte di una strategia finalizzata a respingere gli attori extra-europei per mezzo di un irrigidimento dei confini digitali del vecchio continente.

Sotto il profilo del *Data Nationalism*, il *Data Act* non rappresenta una vera rottura rispetto alla strada già tracciata in precedenza dalla stessa Unione, la quale già da tempo aveva introdotto un meccanismo condizionale per il trasferimento dei dati personali all'estero, ma contribuisce di certo al decremento della fuoriuscita della ulteriore categoria dei dati non personali, che nell'epoca attuale si è dimostrata essere di vitale importanza.

Sebbene l'innalzamento delle barriere digitali europee possa apparire un approccio comprensibile nel contesto storico attuale e possa effettivamente risultare funzionale a un utile posizionamento nello scacchiere globale, la sovranità digitale, specie per una entità tecnologicamente fragile come l'Unione europea, passa anche attraverso due tasselli fondamentali: la riduzione della dipendenza da infrastrutture estere per la gestione dei dati e la cooperazione internazionale finalizzata alla promozione di un approccio comune alla regolazione delle nuove tecnologie[78].

L'Unione dovrebbe pertanto ispirarsi ad una idea di sovranità digitale "aperta" dove riescono a trovare spazio anche partner esterni che sono in grado di fornire quelle competenze e quegli strumenti di cui la realtà continentale attualmente non dispone e deve altresì investire in misura più incisiva sulla effettiva realizzazione di una infrastruttura digitale di matrice europea capace di competere con i concorrenti americani e cinesi. Al contrario, insistere solamente su misure normative ispirate al *Data Nationalism*, trascurando le altre dimensioni rilevanti, non farà altro che alimentare un deleterio "isolazionismo digitale", in cui gli attori

75. Con il primo atto di designazione adottato il 6 settembre 2023, la Commissione europea ha infatti qualificato come *gatekeepers* le seguenti sei piattaforme digitali: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft. Si veda in proposito il comunicato stampa.

76. Ai sensi dell'art. 50, le disposizioni del *Data Act* diverranno applicabili a decorrere dal12 settembre 2025.

77. È bene infatti notare che sia il *Data Act* sia il *Data Governance Act* sono adottati sulla base dell'art. 114 TFUE, che attribuisce al Parlamento ed al Consiglio la competenza normativa per le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno.

78. Aktoudianakis 2020.

pubblici e privati rimangono in un circuito chiuso e non comunicante con l'esterno, il quale, in ultima analisi, non potrà che condurre l'Unione verso una prevedibile disfatta.

Riferimenti bibliografici

A. Aktoudianakis (2020), *Fostering Europe's Strategic Autonomy - Digital sovereignty for growth, rules and cooperation*, in European Policy Centre, 2020

M. Bauer, H. Lee-Makiyama, E. Van der Marel, B. Verschelde (2014), *The cost of data localisation: friendly fire on economic recovery*, ECIPE Occasional Paper No. 3/2014

V. Bertola (2022), *La sovranità digitale e il futuro di Internet*, in "Rivista italiana di informatica e diritto", 2022, n. 1

V. Boncinelli (2021), *Modelli tecnici e disciplina giuridica del c.d. cloud computing*, in "Rivista italiana di informatica e diritto", 2021, n. 1

A. Buratti (2022), *Framing the Facebook Oversight Board: Rough Justice in the Wild Web?* in "Media-Laws", 2022, n. 2

S. Calzolaio (2017), *Protezione dei dati personali*, in R. Bifulco, A. Celotto, M. Olivetti (a cura di), "Digesto delle Discipline Pubblicistiche", Utet giuridica, 2017

K. Cantekin (2018), *Comity upon request. What does the new U.S. CLOUD Act tell us about the future of data flow regulation?*, in "Eurojus.it, Big data and Public Law: new challenges beyond data protection", Numero speciale, 2018

F.H. Cate, C. Kuner, C. Millard, D.J. Svantesson (2014), *Systematic Government Access to Private-Sector Data Redux*, in "International Data Privacy Law", vol. 4, 2014, n. 1

G. Cerrina Feroni (2022), *Luci e ombre della Data Strategy europea*, intervento del 13 maggio 2022 (Doc-Web9769786)

A. Chander, U.P. Lê (2013), *Data Nationalism*, in "Emory Law Journal", vol. 64, 2015, n. 3

D. Castro (2013), *The False Promise of Data Nationalism*, Information Technology & Innovation Foundation, 2013

T. Christakis, F. Terpan (2021), *EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options*, in "International Data Privacy Law", vol. 11, 2021, n. 2, 2021

G. Contaldi (2021), *Il DMA (Digital Markets Act) tra tutela della concorrenza e protezione dei dati personali*, in "Ordine internazionale e diritti umani", 2021, n. 2

S. Couture, S. Toupin (2019), *What does the notion of "sovereignty" mean when referring to the digital?*, in "New Media & Society", vol. 21, 2019, n. 10

R. Creemers (2020), *China's conception of cyber sovereignty: rhetoric and realization*, in D. Broeders, B. van den Berg (eds.), "Governing Cyberspace: Behavior, Power, and Diplomacy. Digital Technologies and Global Politics Lanham", Rowman & Littlefield, 2020

E. Cremona (2021), *L'erompere dei poteri privati nei mercati digitali e le incertezze della regolazione antitrust*, in "Osservatorio sulle fonti", 2021, n. 2

G. Della Morte (2018), *Big Data e Protezione Internazionale Dei Diritti Umani. Regole e Conflitti*, Editoriale Scientifica, 2018

J. Drexl (2016), *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, in "Max Planck Institute for Innovation & Competition", Research Paper No. 16-13, 2016

European Commission (2021), *Inception Impact Assessment*, Ref. Ares(2021)3527151, 28 May 2021

M.F. Ferracane (2017), *Restrictions on cross-border data flows: a taxonomy*, ECIPE working paper, 2017, n. 1

C. Gallese (2022), *A first commentary to the proposal for a new Regulation on fair access and use of data (Data Act)*, in "MediaLaws", 2022, n. 3

G. Gardini (2021), *Le regole dell'informazione. Verso la Gigabit Society*, Giappichelli, 2021

G. Gonzalez Fuster (2014), *The emergence of personal data protection as a fundamental right of the EU*, Springer, 2014

D. Kalff, A. Renda (2019), *Hidden Treasures. Mapping Europe's sources of competitive advantage in doing business*, Centre for European Policy Studies, 2019

W. Kerber (2016), *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, MAGKS Joint Discussion Paper Series in Economics, 2016, n. 37

A. Iannuzzi (2021), *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", 2021, n. 209

M. Martoni (2020), *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in "federalismi.it", 2020, n. 1

M.L. Montagnani (2019), *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in "Mercato concorrenza regole", 2019, n. 2

M. Nino (2013), *Il caso Datagate. I problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in "Diritti umani e diritto internazionale", 2013, n. 3

M. Orofino (2016), *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime*, in "Diritto Pubblico Comparato ed Europeo", 2016, n. 2

V. Pagnanelli (2021), *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in "Rivista italiana di informatica e diritto", 2021, n. 1

J. Pohle, T. Thiel (2020), *Digital sovereignty*, in "Internet Policy Review", vol. 9, 2020, n. 4

D. Polatin-Reuben, J. Wright (2014), *An Internet with BRICS characteristics: data sovereignty and the Balkanisation of the Internet*, Usenix, 2014

C. Polito (2021), *La* governance *globale dei dati e la sovranità digitale europea*, in "IAI Papers", 2021, n. 11

M. Rubechi (2016), *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in "federalismi.it", 2016, n. 23

P.S. Ryan, R. Falvey, S. Merchant (2013), *When the Cloud Goes Local: The Global Problem with Data Localization*, in "Computer", vol. 46, 2013, n. 12

M. Santaniello (2022), *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in "Rivista italiana di informatica e diritto", 2022, n. 1

A. Savelyev (2016), *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, in "Computer Law & Security Review", vol. 32, 2016, n. 1

A. Simoncini (2019), *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in "BioLaw Journal – Rivista di BioDiritto", 2019, n. 1

A. Simoncini (2017), *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino et al. (a cura di), "Diritti e libertà in internet", Le Monnier, 2017

T. Streinz (2021), *The Evolution of European Data Law*, in P. Craig, G. de Búrca (eds.), "The Evolution of EU Law", Oxford University Press, 2021

G. Surblyte (2016), *Data as a Digital Resource*, in "Max Planck Institute for Innovation & Competition Research", Paper No. 16-12, 2016

S. Torregiani (2021), *La circolazione dei dati secondo l'ordinamento giuridico europeo. Il rischio dell'ipertrofia normativa*, in "Rivista italiana di informatica e diritto", 2021, n. 1

S. Torregiani (2021a), *L'impatto dei dati non personali sulle decisioni algoritmiche: la prospettiva delle autorità amministrative indipendenti europee*, in "Osservatorio sulle fonti", 2021, n. 2

S. Torregiani (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in "federalismi.it", 2020, n. 18

J. Van Dijck (2020), *Governing digital societies: Private platforms, public values*, in "Computer Law & Security Review", vol. 36, 2020

J. Van Dijck (2014), *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in "Surveillance and Society", vol. 12, 2014, n. 2

Z. Wang (2012), *Systematic government access to private-sector data*, in "China International Data Privacy Law", vol. 2, 2012, n. 4

A. Wiebe (2016), *Protection of industrial data – a new property right for the digital economy?*, in "Journal of Intellectual Property Law & Practice", 2016

V. Zeno-Zencovich (2016), *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in G. Resta, V. Zeno-Zencovich (a cura di), "La protezione transnazionale dei dati personali. Dai 'Safe Harbour Principles' al 'Privacy Shield'", RomaTre-press, 2016