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

ISSN 2704-7318 • n. 2/2023 • DOI 10.32091/RIID0122 • articolo sottoposto a peer review • pubblicato in anteprima il 19 feb. 2024

Elia Cremona

Quando i dati diventano beni comuni: modelli di *data sharing* e prospettive di riuso

La regolazione europea in materia di dati sembra cambiare paradigma: l'enfasi non è più solo sul profilo della *protezione* e del *controllo*, ma anche della *condivisione*. In questa direzione vanno, in particolare, il *Data Governance Act* e il *Data Act*. Il primo, infatti, promuove il riutilizzo di dati protetti detenuti da enti pubblici, l'intermediazione e il c.d. altruismo dei dati. Il secondo si incentra sui temi dell'accesso ai dati, del diritto di condividere i dati con i terzi e infine sull'obbligo di mettere i dati di soggetti privati a disposizione di enti pubblici per necessità eccezionali. Insomma, la nuova stagione regolatoria europea libera nuovi flussi di dati tra settore pubblico e settore privato (*Business to Government* e *Government to Business*). Il contributo propone una rilettura in chiave critica di tali normative e promuove l'idea dei *data for common good*: un regime speciale per i dati detenuti da soggetti privati ma di pubblico interesse, che vada ad integrare le policy di sostenibilità sociale delle grandi imprese.

Data sharing – Beni comuni – Riuso dei dati – Sostenibilità

When Data Become Commons: Models of Data Sharing and Re-use Perspectives

European data regulation is changing paradigm: the emphasis is no longer only on the profile of protection and control, but also on sharing. In this direction go, in particular, the Data Governance Act and the Data Act. The former, in fact, promotes the reuse of protected data held by public entities, intermediation and so-called altruism of data. The latter focuses on the issues of data access, the right to share data with third parties, and finally the obligation to make data from private entities available to public entities for exceptional needs. In short, the new European regulatory season frees up new data flows between public and private sectors (Business to Government and Government to Business). The paper proposes a critical reinterpretation of these regulations and promotes the idea of data for common good: a special regime for data held by private entities but in the public interest, complementing the social sustainability policies of large companies.

Data sharing – Commons – Data Re-use – Sustainability

L'Autore è assegnista di ricerca in Diritto costituzionale nell'Università degli Studi di Siena

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. Le stagioni della regolazione dei dati: proprietà, controllo, condivisione. – 2. Il riutilizzo dei dati del settore pubblico. – *2.1. La Direttiva* Open Data. – *2.2. Il profilo pubblicistico del* Data Governance Act. – 3. La condivisione e l'accesso ai dati del settore privato. – *3.1. Il profilo privatistico del* Data Governance Act. – *3.2. Il* Digital Services Act *e il* Digital Markets Act. – *3.3. L'*AI Act. – *3.4. Il* Data Act. – *3.5. La Proposta di* Financial Data Access Act. – 4. I dati come beni non rivali nella teoria dei beni comuni. – 5. *Data for Good*: prospettive di *data sharing* per le imprese nel quadro della regolamentazione di sostenibilità.

1. Le stagioni della regolazione dei dati: proprietà, controllo, condivisione

Quando Samuel D. Warren e Louis Brandeis si inventarono il diritto alla privacy[1], inteso – com'è ampiamente noto – nel senso di "right to be let alone", avevano in mente le intrusioni nella vita privata da parte della neonata stampa scandalistica, accusata da parte loro di aver varcato i limiti della decenza e del rispetto del diritto di proprietà[2]. Il diritto alla privacy veniva così coniato come "espansione" del più sacro dei diritti dello stato liberale: la proprietà, appunto, non più considerata come dominio sulle cose connotate da materialità, ma estesa al diritto di impedire la divulgazione di informazioni, pensieri e sentimenti riferibili al soggetto interessato.

Oggi, se pure l'etichetta privacy sia sopravvissuta e ancora largamente impiegata anche nel comune dibattito pubblico, è rimasto ben poco del "diritto ad essere lasciati soli". Anzi, il principale campo di applicazione della normativa c.d. privacy è quello delle relazioni sociali nello spazio digitale, nel quale l'*animus* dell'utente medio è non già quello di escludere qualcuno dal proprio dominio (*excludendi*) bensì di condividere (*communicandi*) informazioni, pensieri e sentimenti che lo riguardano con una platea più ampia possibile di soggetti. Ciò si verifica sia nell'ipotesi in cui la condivisione del dato è lo scopo diretto dell'utente sul web, come nel caso delle piattaforme social (*Instagram*, *X*, *Facebook*), sia quando la condivisione è invece strumentale all'accesso ad un servizio, come nel caso dei servizi "gratuiti" di cui fruiamo quotidianamente attraverso internet (dalla galassia dei servizi Google ai software Microsoft, fino ai più recenti sistemi di intelligenza artificiale generativa come *Chat-GPT*): per quanto il grado di consapevolezza medio dell'effetto "sorveglianza" che questa fruizione gratuita produce sia ancora molto scarso, soprattutto nelle generazioni più giovani, non si può dubitare del fatto che nello spazio digitale la privacy, tradizionalmente intesa, sia divenuta un problema recessivo[3].

1. Il riferimento è al noto Warren-Brandeis 1890, pp. 193-220.
2. *Ivi*, p. 196: «the press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and the vicious, but has become a trade. […] To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers».
3. Sull'alternativa tra pagamento di un prezzo e cessione dei dati personali, si veda la recente decisione di Meta di sottoporre la scelta ai propri utenti europei. A fine ottobre 2023, infatti, è comparso sugli schermi degli utenti questo avviso: «Per ottemperare alle normative europee in continua evoluzione stiamo introducendo la possibilità di sottoscrivere un abbonamento in Ue, See e in Svizzera. A novembre offriremo alle persone che utilizzano Facebook o Instagram che risiedono in queste regioni la possibilità di continuare a utilizzare questi servizi personalizzati gratuitamente con la pubblicità, oppure di sottoscrivere un abbonamento per non visualizzare

L'evoluzione dei costumi sociali è così "ruotata" intorno al concetto di privacy, che sul piano giuridico è però rimasto per lungo tempo ancorato alla cultura proprietaria che lo aveva ispirato.

Volendo scandire le tappe essenziali di questo percorso di affrancamento dal modello proprietario, possiamo – sul piano costituzionale e del diritto europeo – indicare questa sequenza di atti: la Convenzione Europea dei Diritti dell'Uomo, la Direttiva 95/46/CE, la Carta di Nizza, il GDPR e, da ultimo, il corposo pacchetto di atti con i quali l'Unione europea ha disciplinato il fenomeno digitale.

In via di sintesi: il citato modello proprietario ha prodotto sul piano normativo l'affermazione del diritto al rispetto della vita privata e familiare, postulato in ambito convenzionale dall'art. 8 della CEDU e ribadito all'art. 7 della Carta di Nizza. A questo si è affiancato, dapprima con la Direttiva 95/46/CE[4], poi con l'art. 8 della Carta di Nizza, l'art. 16 del TFUE e infine con il GDPR, il paradigma del "controllo" e della "protezione dei dati", non più inteso in senso assolutistico quale proiezione di un diritto di proprietà, ma quale punto di caduta del bilanciamento tra l'esigenza di tutelare un diritto fondamentale della personalità con l'opposta esigenza di garantire quanto più possibile la "circolazione" dei dati, personali e non personali.

Diversamente dalla comune vulgata[5], il GDPR ha sin da subito rappresentato un compromesso

più le inserzioni. Le informazioni delle persone che decideranno di sottoscrivere l'abbonamento non saranno utilizzate per gli annunci pubblicitari. […] A seconda che si scelga di attivare l'abbonamento sul web o da mobile il costo sarà rispettivamente di 9,99 euro al mese sul web o di 12,99 euro al mese su iOS e Android». La conformazione dell'avviso suggeriva, con la solita tecnica di *nudging* consistente in una colorazione più *catchy* del relativo bottone, la scelta per il servizio gratuito. Ciò a dimostrazione del fatto che Meta non ha alcuna intenzione di cambiare il proprio *business model*. Questa mossa è stata in realtà la risposta alla decisione, urgente e vincolante *ex* art. 66 GDPR, adottata il 27 ottobre 2023 dall'*European Data Protection Board* (EDPB) che aveva imposto di acquisire il consenso degli utenti per il c.d. *behavioural advertising*. A questa è seguita, il 10 novembre 2023, la decisione finale dell'Autorità irlandese che ha conseguentemente imposto il divieto di trattamento. Nelle due settimane intercorrenti tra i due provvedimenti, però, Meta aveva già sottoposto a tutti i propri utenti europei la scelta tra consenso al trattamento per fini di pubblicità comportamentale e pagamento di un prezzo. Non è irragionevole pensare che la percentuale di coloro che hanno scelto di abbonarsi sia risibile e che dunque, nell'arco di qualche giorno, Meta possa avere acquisito il consenso di qualche centinaio di milioni di persone. Non è questa la sede per ulteriori approfondimenti, ma due osservazioni possono farsi sin d'ora. La prima è che la modalità di acquisizione del consenso da parte di Meta si è rivelata particolarmente aggressiva: l'utente si è trovato improvvisamente a dover scegliere tra dare il consenso e pagare una somma di oltre 100 € all'anno, molto rilevante per il mercato di riferimento (le altre piattaforme social sono quasi tutte gratuite, mentre per X si parla dell'introduzione di un abbonamento di 1 dollaro all'anno). Questo può far pensare sia ad un possibile illecito antitrust, sulla falsariga di quello sanzionato dal *Bundeskartellamt* per illegittima compressione della libertà di scelta del consumatore (*fehlende Wahlmöglichkeit*), sia ad una possibile pratica commerciale scorretta, forse pure di tipo aggressivo. Sulla vicenda tedesca, si veda Pardolesi-Van den Bergh-Weber 2020, pp. 518-519; Davola 2021, p. 65. Le impugnazioni in sede giudiziaria del provvedimento hanno occasionato, com'è noto, l'importante sentenza CGUE, 4 luglio 2023, in causa C-252/21, *Meta platforms e a.* (condizioni generali d'uso di un social network), ECLI:EU:C:2023:537. Per un commento, v. Bachelet 2023. La seconda considerazione che può accennarsi è poi di carattere generale: la velocità – e la facilità – con la quale Meta ha formalmente ottemperato al parere vincolante dell'EDPB, di nuovo grazie al consenso (dis)informato degli utenti, dimostra ancora una volta la debolezza della regolazione europea di fronte allo strapotere – di fatto – delle grandi piattaforme nello spazio digitale. Anzi, recuperando le intuizioni di Pistor 2019, quel che emerge è piuttosto l'uso della legislazione proprio come strumento di consolidamento del potere di queste grandi piattaforme digitali. Cfr. in tema Sandulli 2021.

4. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
5. Cfr. Commissione europea 2020.

tra le esigenze del mercato dei dati e quello della tutela dei diritti[6], delineando uno statuto giuridico dei dati personali per lo più *funzionale* al consolidamento e al corretto funzionamento del mercato unico e, solo in parte, *strumentale* alla garanzia delle libertà fondamentali dell'Unione[7].

Dopodiché, il processo non si è arrestato e il concetto giuridico di "dato" ha iniziato a "spersonalizzarsi", in un'ottica sempre più funzionale all'integrazione del mercato unico[8]. A partire dal 2017, l'Unione ha avviato un ampio processo di riforma che si è incentrato sul tema dell'apertura dei dati e il riutilizzo delle informazioni del settore pubblico (flussi *Government to Government*, c.d. G2G, e *Government to Business*, c.d. G2B)[9]. Dopodiché, le tappe sono state scandite dall'approvazione, nel 2018, del Regolamento sulla circolazione dei dati non personali[10] e poi dalla pubblicazione della *Strategia europea per i dati* del febbraio 2020[11], che ha gettato le basi, tra gli altri, per il *Data Governance Act*[12] (che per primo definisce il "dato" in quanto tale[13]) e il *Data Act*[14]. In particolare, l'Unione ha annunciato la creazione di spazi comuni europei di dati[15] in alcuni settori strategici[16], non rinunciando ad incoraggiare – ed è questo il profilo su cui ci si soffermerà in chiusura – lo sblocco di flussi di dati dal settore privato a quello pubblico (*Business to Government*,

6. Si è sostenuto altrove che tale compromesso si è risolto forse più a vantaggio dei protagonisti dei mercati digitali che degli utenti, spesso inconsapevoli sia della compressione dei propri diritti riconosciuti dal GDPR che degli strumenti di tutela, largamente inattivati. Cfr. Cremona 2023, p. 105 ss.
7. Cfr. De Gregorio-Paolucci 2022, p. 113. Tale profilo emerge abbastanza chiaramente già dai considerando della Direttiva del 1995, ma anche dalla Direttiva 2000/31/EC relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico").
8. Cfr. Zech 2015, p. 192; De Franceschi-Lehmann 2015.
9. Tale processo ha condotto all'adozione della Direttiva UE 2019/1024, c.d. Direttiva *Open Data*. Nel 2017, infatti, la Commissione europea aveva aperto una consultazione pubblica sulla revisione della direttiva 2013/37/UE, che a sua volta aveva modificato la direttiva 2003/98/CE in tema *Public Sector Information*.
10. 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. Cfr. Galiano-Leogrande-Massari-Massaro 2020, p. 63.
11. Commissione europea, *Una strategia europea per i dati*, COM(2020) 66, del 19 febbraio 2020. Cfr. anche European Data Protection Supervisor 2020, p. 4.
12. 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.
13. Ai sensi dell'art. 2, par. 1, n. 1), del *Data Governance Act* appartiene alla definizione di dati «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».
14. Al momento in cui si scrive, il *Data Act* è stato definitivamente approvato ed è in attesa di pubblicazione sulla Gazzetta Ufficiale dell'Unione europea.
15. Gli spazi comuni europei dei dati riuniscono le infrastrutture di dati e i quadri di governance pertinenti al fine di facilitare la messa in comune e la condivisione dei dati. In particolare essi (i) implementano strumenti e servizi di condivisione dei dati per la raccolta, l'elaborazione e la condivisione dei dati da parte di un numero aperto di organizzazioni e uniscono capacità *cloud* efficienti dal punto di vista energetico e affidabili e servizi correlati; (ii) includono strutture di governance dei dati, compatibili con la pertinente legislazione dell'Ue, che determinano, in modo trasparente ed equo, i diritti di accesso e trattamento dei dati; (iii) migliorano la disponibilità, la qualità e l'interoperabilità dei dati, sia in contesti specifici che tra settori diversi. V. Commissione europea, *Commission staff working document on Common European Data Spaces*, SWD(2022) 45 final, 23 February 2022.
16. Sanità, agricoltura, manifattura, energia, mobilità, finanza, pubblica amministrazione, competenze, *cloud* europeo per la scienza aperta e soddisfacimento degli obiettivi del Green Deal. A questi si sono poi aggiunti altri settori importanti come quello dei media e del patrimonio culturale. L'obiettivo finale perseguito è che, insieme, gli spazi di dati formino uno spazio unico europeo, un vero mercato unico dei dati.

c.d. B2G)[17] e tra privati (*Business to Business*, c.d. B2B, e *Business to Consumer*, c.d. B2C)[18].

Dunque, quel che si va verificando nelle pagine seguenti è se non sia appena stato compiuto, nel campo regolatorio europeo, un passo *definitivo* nel processo di allontanamento dal paradigma proprietario che ha caratterizzato la prima (*right to be let alone*) e, in parte, la seconda stagione (*protezione e controllo*) della normativa privacy. In particolare, ci si chiederà se non siamo entrati in una (terza) fase regolatoria caratterizzata da un accento sul tema della "condivisione"[19], che mira a "liberare" enormi quantità di dati a beneficio del mercato unico e, auspicabilmente, anche della collettività.

2. Il riutilizzo dei dati del settore pubblico

La presa di consapevolezza sulle potenzialità derivanti dalla condivisione dei dati ha come primo punto di emersione, come si accennava, la previsione di una disciplina di apertura dei dati e riuso delle informazioni del settore *pubblico*. Questo, come vedremo, si spiega secondo una logica molto semplice: mentre i dati del settore privato costituiscono generalmente un *asset* patrimoniale strumentale all'esercizio dell'attività d'impresa, secondo le logiche della concorrenza e della rivalità, viceversa i dati nella disponibilità dei soggetti pubblici non soggiacciono – di norma – a logiche di mercato. In altre parole, se la condivisione e il riuso dei dati nel settore privato si scontrano con le dinamiche dei vantaggi e degli svantaggi competitivi, nel settore pubblico la stessa operazione di "messa a disposizione" dei dati a soggetti terzi (pubblici o anche privati) assume i contorni di una esternalità positiva, ovvero di una azione non specificamente remunerata che produce di per sé effetti positivi sull'economia o sull'attività di altri soggetti.

2.1. La Direttiva *Open Data*

Esattamente a questa logica è ispirata la Direttiva *Open Data* 2019/1024[20] che ha stabilito le regole per l'accesso e l'utilizzo dei dati pubblici da parte delle organizzazioni pubbliche e private all'interno dell'Ue. La direttiva muove da alcune considerazioni che è qui utile riproporre: «il *settore pubblico* degli Stati membri *raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni* in molti settori di attività, per esempio informazioni di tipo sociale, politico, economico, giuridico, geografico, ambientale, meteorologico, sismico, turistico, informazioni in materia di affari, di brevetti e di istruzione. […] La *fornitura di tali informazioni* […] consente ai cittadini e alle persone giuridiche di *individuare nuovi modi di utilizzarle e di creare prodotti e servizi nuovi e innovativi*»[21]. E ancora più chiaramente: «*l'informazione del settore pubblico* rappresenta una fonte straordinaria di dati *in grado di contribuire a migliorare il mercato interno e lo sviluppo di nuove applicazioni per i consumatori e le persone giuridiche*. L'utilizzo intelligente dei dati, ivi compreso il loro trattamento attraverso applicazioni di intelligenza artificiale, può *trasformare tutti i settori dell'economia*»[22].

Per conseguenza, la direttiva fissa un *Principio generale* (art. 3) per il quale i "documenti" in possesso di enti pubblici e imprese pubbliche siano riutilizzabili «a fini commerciali o non commerciali»[23],

17. Commissione europea 2020.
18. Commissione europea 2019.
19. Il concetto di condivisione, come si vedrà *infra*, va distinto dalla mera circolazione. Sebbene non vi sia una definizione di "circolazione" nel GDPR, questa si differenzia dalla "condivisione", definita come segue all'art. 2, par. 1, n. 10), del Regolamento UE 2022/868 (*Data Governance Act*): «la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito».
20. La Direttiva *Open Data* dell'Unione europea (EU) 2019/1024 è stata recepita in Italia dal d.lgs. n. 200/2021 che ha emendato il d.lgs. 36/2006.
21. Considerando n. 8, nostro il corsivo.
22. Considerando n. 9, nostro il corsivo.
23. Art. 3 (*Principio generale)*: «1. Fatto salvo il paragrafo 2 del presente articolo, gli Stati membri provvedono affinché i documenti cui si applica la presente direttiva in conformità dell'articolo 1 siano riutilizzabili a fini

siano messi a disposizione in un «lasso di tempo ragionevole» (art. 4)[24] a titolo, di regola, gratuito (art. 6)[25], sempre salvo il rispetto della normativa in materia di protezione dei dati personali, di diritto d'autore e di proprietà industriale.

2.2. Il profilo pubblicistico del *Data Governance Act*

Con il *Data Governance Act*[26], definitivamente applicabile nell'Unione dal 24 settembre 2023, la logica del riutilizzo dei dati pubblici viene ulteriormente sviluppata, anche muovendo dalla constatazione degli scarsi risultati prodotti su questo piano dalla Direttiva *Open Data*: «talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, *spesso non sono messe a disposizione*, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, *nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile*»[27].

Il Regolamento perciò mira, nella sua parte dedicata al settore pubblico, a sbloccare quelle particolari categorie di dati soggetti a regimi speciali che ne impedivano la riutilizzazione[28], incoraggiando l'adozione di tecniche di anonimizzazione, aggregazione *et al.* dei dati protetti in maniera tale da assicurare il pieno rispetto dei diritti di terzi[29].

commerciali o non commerciali conformemente ai capi III e IV. 2. Gli Stati membri provvedono affinché i documenti i cui diritti di proprietà intellettuale sono detenuti da biblioteche, comprese le biblioteche universitarie, musei e archivi, e i documenti in possesso delle imprese pubbliche siano riutilizzabili a fini commerciali o non commerciali, qualora il loro riutilizzo sia autorizzato, conformemente ai capi III e IV».

24. Art. 4 (*Trattamento delle richieste di riutilizzo)*: «1. Gli enti pubblici esaminano le richieste di riutilizzo e mettono i documenti a disposizione del richiedente, ove possibile e opportuno per via elettronica o, se è necessaria una licenza, mettono a punto l'offerta di licenza per il richiedente entro un lasso di tempo ragionevole e coerente con quello previsto per l'esame delle richieste di accesso ai documenti».
25. Art. 6 (*Principi di tariffazione)*: «1. Il riutilizzo di documenti è gratuito. Tuttavia, può essere autorizzato il recupero dei costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato. 2. In via eccezionale il paragrafo 1 non si applica: a) a enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico; b) a biblioteche, comprese le biblioteche universitarie, musei e archivi; c) alle imprese pubbliche […]».
26. 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").
27. Considerando n. 6, nostro il corsivo, ove si ribadisce che «l'idea che i dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società è da tempo parte integrante delle politiche dell'Unione. La direttiva (UE) 2019/1024 e la normativa settoriale dell'Unione garantiscono che gli enti pubblici rendano facilmente disponibile per l'utilizzo e il riutilizzo una quota maggiore dei dati che producono».
28. *Ivi*: «A causa della sensibilità di tali dati, prima che essi siano messi a disposizione si devono soddisfare alcuni requisiti procedurali tecnici e giuridici al fine, se non altro, di garantire il rispetto dei diritti di terzi sui dati in questione o di limitare l'effetto negativo sui diritti fondamentali, sul principio di non discriminazione e sulla protezione dei dati. L'adempimento di tali requisiti risulta abitualmente molto dispendioso in termini di tempo e richiede un livello molto elevato di conoscenze. Ciò ha determinato un utilizzo insufficiente di tali dati. Per quanto alcuni Stati membri stiano istituendo strutture, procedure o adottando norme per agevolare tale tipo di riutilizzo, ciò non accade in tutta l'Unione. Al fine di agevolare l'utilizzo dei dati per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati, sono necessarie condizioni chiare per l'accesso a tali dati e il loro utilizzo in tutta l'Unione».
29. Considerando n. 7: «Esistono tecniche che consentono l'analisi di banche dati contenenti dati personali, quali l'anonimizzazione, la privacy differenziale, la generalizzazione, la soppressione e la casualizzazione, l'utilizzo di dati sintetici o metodi analoghi, nonché altri metodi all'avanguardia di tutela della vita privata che potrebbero contribuire a

Il *Data Governance Act*, come accennato, fornisce per la prima volta alcune importanti definizioni, relative ai concetti di "dato"[30], di "riutilizzo" del dato pubblico[31], di "titolare dei dati"[32], di "utente dei dati"[33] e di "condivisione dei dati"[34].

Per quanto concerne il profilo pubblicistico, il Regolamento disciplina (art. 5) le condizioni per il riutilizzo di una o più delle categorie di dati protetti *ex* art. 3, par. 1[35], detenute da enti pubblici, prescrivendo che esse siano pubbliche, non discriminatorie, trasparenti, proporzionate e oggettivamente giustificate in relazione alle categorie di dati e alle finalità del riutilizzo e alla natura dei dati per i quali è consentito il riutilizzo. In ogni caso, tali condizioni non debbono «limitare la concorrenza»[36]. Il Regolamento prevede (art. 6) che gli enti pubblici che consentono il riutilizzo delle categorie di dati protetti di cui sopra possano imporre tariffe non discriminatorie, proporzionate, oggettivamente giustificate (in particolare, per l'eventuale trattamento applicato al fine di garantire i diritti dei terzi; *e.g.,* anonimizzazione, aggregazione etc.) e che non limitino il gioco concorrenziale. La gestione è

un trattamento dei dati maggiormente rispettoso della vita privata. Gli Stati membri dovrebbero fornire sostegno agli enti pubblici affinché utilizzino in maniera ottimale tali tecniche, rendendo così disponibili quanti più dati possibili per la condivisione. L'applicazione di tali tecniche, unite a valutazioni d'impatto globali in materia di protezione dei dati e ad altre tutele può contribuire a una maggiore sicurezza nell'utilizzo e riutilizzo dei dati personali e dovrebbe garantire il riutilizzo sicuro dei dati commerciali riservati a fini statistici, di ricerca e di innovazione. […]».

30. Art. 2, par. 1, n. 1): «"dati": qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».
31. Art. 2, par. 1, n. 2): «"riutilizzo": l'utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico».
32. Art. 2, par. 1, n. 8): «"titolare dei dati": una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli».
33. Art. 2, par. 1, n. 9): «"utente dei dati": una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali».
34. Art. 2, par. 1, n. 10): «"condivisione dei dati": la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito».
35. Ai sensi dell'art. 3, par. 1, si tratta dei dati protetti per: a) riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; b) riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; o d) protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024.
36. Ai sensi del par. 3 dell'art. 5, «Gli enti pubblici garantiscono, conformemente al diritto dell'Unione e nazionale, la tutela della natura protetta dei dati. Essi garantiscono il rispetto dei requisiti seguenti: a) concedere l'accesso per il riutilizzo dei dati soltanto qualora l'ente pubblico o l'organismo competente abbia garantito, in seguito alla richiesta di riutilizzo, che i dati sono stati: i) anonimizzati, nel caso di dati personali; e ii) modificati, aggregati o trattati mediante qualsiasi altro metodo di controllo della divulgazione, nel caso di informazioni commerciali riservate, compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale; b) accedere ai dati e riutilizzare gli stessi da remoto all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico; c) accedere ai dati e riutilizzare gli stessi all'interno dei locali fisici in cui si trova l'ambiente di trattamento sicuro, rispettando rigorose norme di sicurezza, a condizione che l'accesso remoto non possa essere consentito senza compromettere i diritti e gli interessi di terzi».

affidata ad un sistema di sportelli unici (art. 8), con articolazione settoriale, regionale o locale.

Ad ogni modo, è opportuno chiarire che il Regolamento non fissa alcun obbligo per gli enti pubblici di acconsentire al riutilizzo dei dati, ma stabilisce una serie di regole comuni che debbono applicarsi qualora l'ente, sia pure dietro compenso, decida di consentirne l'utilizzo.

L'ente pubblico può inoltre svolgere attività di fornitura di "servizi di intermediazione dei dati", nei termini di cui si dirà *infra*, e rivestire altresì il ruolo di "titolare dei dati" ai sensi del Regolamento, ovvero di quel soggetto a cui l'interessato può richiedere di mettere i propri dati, siano essi personali o non personali, a disposizione di un soggetto terzo, "utente dei dati", che ha diritto di utilizzarli per finalità commerciali o non commerciali[37].

3. La condivisione e l'accesso ai dati del settore privato

Si è detto che la recente regolazione europea mira a liberare enormi quantità di dati a beneficio del mercato e dunque a favorire quanto più possibile la loro circolazione e condivisione nel rispetto dei diritti dei soggetti interessati e dei terzi a vario titolo coinvolti. Con molta più prudenza rispetto a quanto osservato per il settore pubblico, la disciplina di favore per la condivisione e l'accesso ai dati coinvolge anche il settore privato. In particolare, come si vedrà in appresso, l'Unione ha varato per lo più norme incentivanti la condivisione volontaria dei dati e solo in rare ed eccezionali occasioni ha previsto formule cogenti di accesso ai dati da parte dei soggetti pubblici o di soggetti terzi del mercato.

3.1. Il profilo privatistico del *Data Governance Act*

Proseguendo la nostra disamina, muoviamo verso il lato privatistico del *Data Governance Act*. In particolare, le fattispecie rilevanti sono quelle dei "servizi di intermediazione dei dati"[38] e dell'"altruismo dei dati"[39].

Con riferimento ai primi, si tratta di attività di intermediazione volta a far instaurare rapporti *commerciali* di condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e utenti dei dati, dall'altro (Capo III del Regolamento).

Diversamente, l'altruismo dei dati mira a favorire la condivisione volontaria di dati *senza compenso* (salvo il rimborso dei costi sostenuti)

37. Ciò può avvenire sia nell'ambito di una "intermediazione dei dati" di cui al Capo III del Regolamento, sia nell'ambito dell'"altruismo dei dati" di cui al Capo IV, di cui si dirà *infra*.

38. Art. 2, par. 1, n. 11): «"servizio di intermediazione dei dati": un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali, ad esclusione almeno di: a) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; b) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; c) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; d) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali».

39. Art. 2, par. 1, n. 16): «"altruismo dei dati": la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

per obiettivi di interesse generale (Capo IV del Regolamento).

In entrambi i casi, il cuore della proposta è la condivisione dei dati secondo la logica della non rivalità e secondo il metodo della volontarietà: il regolamento non introduce, come accennato già per il settore pubblico, alcun obbligo di condivisione[40], ma promuove e regolamenta le forme attraverso le quali tale condivisione può realizzarsi. In particolare, regole stringenti sono fornite in merito alle *Condizioni per la fornitura di servizi di intermediazione dei dati* (art. 12) e ai *Requisiti generali per la registrazione in un registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute* (artt. 17 ss.).

L'obiettivo a tendere di questa legislazione di favore per la condivisione è perciò quello della creazione di "spazi comuni europei di dati", di cui si accennava, ossia «quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile»[41].

3.2. Il *Digital Services Act* e il *Digital Markets Act*

Non a una logica di condivisione, ma di "accessibilità", risponde la disciplina prevista nel *Digital Services Act*[42] e nel *Digital Markets Act*[43]. Come noto, i due regolamenti varati dall'Unione nel 2022 hanno come obiettivo la regolazione delle grandi piattaforme digitali, il primo nell'ottica di assicurare responsabilità e trasparenza dei prestatori di servizi di intermediazione online e il secondo nell'ottica di regolamentare *ex ante* il comportamento di mercato delle imprese che forniscono servizi di piattaforma di base, c.d. *gatekeeper*. Senza pretesa alcuna di voler qui sintetizzare la complessa disciplina prevista dai due corposi regolamenti (pienamente applicabili a partire da febbraio e marzo 2024), si può qui osservare – ai nostri fini – quanto segue.

Quel che emerge è un regime tutt'affatto speciale per i dati delle imprese che rientrano nell'ambito soggettivo di applicazione di queste due normative: i dati sono sì *asset* patrimoniali dell'impresa (dunque regolarmente protetti dalle normative in materia di proprietà, *data protection* e segretezza commerciale) ma "accessibili" da un numero chiuso di soggetti che vengono puntualmente indicati.

Per quanto riguarda il DSA, l'art. 40 prevede la possibilità per il Coordinatore dei servizi digitali del luogo di stabilimento o la Commissione di chiedere l'accesso o la comunicazione di dati specifici, compresi i dati relativi ai sistemi algoritmici. Tale richiesta può comprendere, ad esempio, i dati necessari a valutare i rischi e gli eventuali danni derivanti dai sistemi delle *Very Large Online Platforms*, i dati relativi alla precisione, al funzionamento e alle prove dei sistemi algoritmici per la moderazione dei contenuti, dei sistemi di raccomandazione o dei sistemi pubblicitari, compresi, se del caso, i dati

40. Si veda il considerando n. 27: «si prevede che i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati. I servizi di intermediazione dei dati specializzati, che sono indipendenti dagli interessati, dai titolari dei dati e dagli utenti dei dati, potrebbero facilitare l'emergere di nuovi ecosistemi basati sui dati indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato, prevedendo nel contempo un accesso non discriminatorio all'economia dei dati per le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati. […]».

41. *Ibidem*.

42. 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.

43. 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.

di addestramento e gli algoritmi, oppure i dati sui processi e i risultati dei sistemi di moderazione dei contenuti o dei sistemi interni di gestione dei reclami. L'accesso ai dati è altresì riconosciuto ai ricercatori abilitati[44] allo scopo di condurre ricerche che contribuiscano al rilevamento, all'individuazione e alla comprensione dei rischi sistemici nell'Unione[45] e per la valutazione dell'adeguatezza, dell'efficienza e degli impatti delle misure di attenuazione dei rischi[46].

Per quanto riguarda invece il DMA, l'accesso ai dati detenuti dai *gatekeeper* non è solamente garantito – senza particolari limitazioni – alla Commissione nell'ambito dei poteri di indagine di cui all'art. 21 del Regolamento[47], ma è altresì assicurato agli "utenti commerciali"[48]. In particolare, ai sensi dell'art. 6, par. 10, il *gatekeeper* è tenuto a fornire a titolo gratuito agli utenti commerciali e a terzi autorizzati da un utente commerciale, su richiesta, «un accesso efficace, di elevata qualità, continuo e in tempo reale a dati aggregati e non aggregati, compresi i dati personali», garantendo alle stesse condizioni «l'uso di tali dati, che sono forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base […] da parte di tali utenti commerciali e degli utenti finali che si avvalgono di prodotti o servizi forniti da tali utenti commerciali».

Non solo, sempre ai sensi dell'art. 6, ma par. 11, alcuni dei dati in possesso dei *gatekeeper* ricevono una disciplina sostanzialmente equiparabile a quella di una *essential facility*[49], prevedendosi che il gatekeeper garantisca alle imprese terze che forniscono motori di ricerca online, su loro richiesta, «l'accesso a condizioni eque, ragionevoli e non discriminatorie a dati relativi a posizionamento, ricerca, click e visualizzazione per quanto concerne le ricerche gratuite e a pagamento generate dagli utenti finali sui suoi motori di ricerca online»[50].

3.3. L'*AI Act*

Similmente, anche la proposta di *AI Act*[51] (nella versione aggiornata agli emendamenti proposti dal Parlamento europeo del giugno 2023) fa riferimento alle opportunità generate dalla condivisione dei dati per la formazione, la convalida e la sperimentazione di sistemi di intelligenza artificiale[52].

44. Ai sensi del par. 8 dell'art. 40.
45. Come stabilito a norma dell'articolo 34, paragrafo 1.
46. A norma dell'articolo 35.
47. Cfr. il considerando n. 81, a mente del quale: «È opportuno conferire alla Commissione il potere di richiedere le informazioni necessarie ai fini del presente regolamento. La Commissione dovrebbe in particolare avere accesso a tutti i pertinenti documenti, dati, banche dati, algoritmi e informazioni necessari per avviare e svolgere indagini e per monitorare l'osservanza degli obblighi sanciti dal presente regolamento, a prescindere da chi sia in possesso di tali informazioni, e indipendentemente dalla loro forma o formato, dal supporto su cui sono conservati o dal luogo in cui sono conservati».
48. Ai sensi dell'art. 2, par. 1, n. 21), è utente commerciale «qualsiasi persona fisica o giuridica che, nell'ambito delle proprie attività commerciali o professionali, utilizza i servizi di piattaforma di base ai fini della fornitura di beni o servizi agli utenti finali o nello svolgimento di tale attività».
49. Cfr. *ex multis*, Graef 2016.
50. Non troppo dissimile dall'obbligo di garantire l'accesso ai dati di cui all'art. 6, parr. 10 e 11, è l'obbligo di fornitura di "informazioni" sugli annunci pubblicitari di cui all'art. 5, parr. 9 e 10.
51. Al momento in cui si scrive non è ancora noto il testo definitivo sul quale il 9 dicembre 2023 è stato raggiunto l'accordo politico tra Parlamento e Consiglio e che sarà oggetto di adozione formale da parte dei due organi.
52. Cfr. il considerando n. 45 della versione sopra citata della proposta: «per lo sviluppo e la valutazione dei sistemi di intelligenza artificiale ad alto rischio, è opportuno che alcuni soggetti, come i fornitori, gli organismi notificati e altre entità pertinenti, come i poli di innovazione digitale, le strutture di sperimentazione e i ricercatori, possano accedere e utilizzare serie di dati di alta qualità nell'ambito dei rispettivi settori di attività connessi al presente regolamento. Gli spazi comuni di dati europei istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra le imprese e con le amministrazioni pubbliche nell'interesse pubblico saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di alta qualità per la formazione,

Il Regolamento, la cui versione finale – si ribadisce – non è ancora nota, prevede altresì meccanismi eccezionali di accesso, per così dire "invertito" (cioè da pubblico a privato), funzionali ad assicurare la vigilanza sul rispetto della normativa in materia di sistemi di intelligenza artificiale ad alto rischio: l'autorità nazionale di vigilanza potrà accedere, previa richiesta motivata sotto il profilo della necessarietà, «agli insiemi di dati relativi alla formazione, alla convalida e ai test utilizzati dal fornitore o, se del caso, dall'implementatore» (art. 64 della Proposta).

3.4. Il *Data Act*

Il *Data Act* rappresenta senz'altro il testo normativo più avanzato sul tema dell'accesso e della condivisione dei dati[53]. Il Regolamento persegue diverse finalità d'interesse per quanto qui ci occupa, muovendo dall'idea di rimuovere quanto più possibile gli ostacoli all'accesso e alla condivisione dei dati tra consumatori e imprese, tra imprese, e – a certe condizioni – tra imprese e settore pubblico[54]. Innanzitutto, il Regolamento garantisce che gli utenti[55] di un prodotto connesso[56] o di un servizio correlato[57] (solitamente chiamati "IoT", *Internet of Things*[58]) possano accedere tempestivamente ai

la convalida e la sperimentazione dei sistemi di IA. Ad esempio, nel settore sanitario, lo spazio europeo dei dati sanitari faciliterà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di intelligenza artificiale su tali insiemi di dati, in modo rispettoso della privacy, sicuro, tempestivo, trasparente e affidabile, e con un'adeguata governance istituzionale. Le autorità competenti, comprese quelle settoriali, che forniscono o supportano l'accesso ai dati possono anche sostenere la fornitura di dati di alta qualità per l'addestramento, la convalida e il test dei sistemi di intelligenza artificiale».

53. Si fa riferimento al testo approvato formalmente dal Parlamento Europeo il 9 novembre 2023 e dal Consiglio il 27 novembre 2023, che è in attesa di pubblicazione sulla Gazzetta Ufficiale dell'Unione europea.
54. V. considerando n. 2: «Gli ostacoli alla condivisione dei dati impediscono un'allocazione ottimale dei dati a vantaggio della società. Tali ostacoli comprendono la mancanza di incentivi per i titolari dei dati a stipulare volontariamente accordi di condivisione dei dati, l'incertezza sui diritti e gli obblighi in relazione ai dati, i costi per la conclusione di contratti e l'implementazione di interfacce tecniche, l'elevato livello di frammentazione delle informazioni in silos di dati, la cattiva gestione dei metadati, l'assenza di norme per l'interoperabilità semantica e tecnica, le strozzature che impediscono l'accesso ai dati, la mancanza di prassi comuni di condivisione dei dati e l'abuso degli squilibri contrattuali per quanto riguarda l'accesso ai dati e il loro uso».
55. Ai sensi dell'art. 2, par. 1, n. 12) è definito "utente": «una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato».
56. Ai sensi dell'art. 2, par. 1, n. 5) è definito "prodotto connesso": «un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente».
57. Ai sensi dell'art. 2, par. 1, n. 6) è definito "servizio correlato": «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».
58. L'espressione *Internet of Things* si ritiene sia stata formulata per la prima volta nel 1999, con riferimento ai dispositivi RFId (*Radio Frequency Identification*), dall'ingegnere inglese Kevin Ahston, cofondatore dell'Auto-ID Center di Massachussetts; cfr. Ashton 2009. L'IoT si declina pressoché in ogni settore dell'economia: si parla oggi di *smart agriculture* (consistente nel monitoraggio di parametri micro-climatici a supporto dell'agricoltura al fine di migliorare la qualità dei prodotti, ridurre le risorse utilizzate e l'impatto ambientale), di *smart cars* (ovvero la connessione delle auto per comunicare informazioni in tempo reale al consumatore, connessione tra veicoli o tra questi e l'infrastruttura circostante per la prevenzione e la rivelazione degli incidenti), *smart cities* (cioè l'attività di monitoraggio e gestione dei servizi pubblici di una città, come il trasporto pubblico, l'igiene

dati generati dall'uso di tale prodotto[59] o servizio[60] e che possano utilizzare tali dati. Agli utenti è riconosciuto il "diritto" (art. 5)[61] di condividerli con terzi di loro scelta, con conseguente obbligo per i titolari dei dati[62] di metterli a disposizione.

Il Regolamento garantisce inoltre che i titolari dei dati mettano i dati a disposizione dei destinatari dei dati[63] nell'Unione a condizioni eque, ragionevoli e non discriminatorie e in modo trasparente (art. 8), prevedendo pertanto specifiche norme di diritto contrattuale volte a impedire lo sfruttamento degli squilibri contrattuali che ostacolano l'accesso equo ai dati e il loro utilizzo (artt. 13 ss.).

Infine, una delle disposizioni più interessanti e significative è quella che assicura un flusso coattivo di dati dal settore privato al settore pubblico (B2G), in caso di necessità eccezionali[64]. Ai sensi dell'art. 14, infatti, i titolari dei dati sono tenuti a mettere 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 uno specifico compito di pubblico interesse. Tale forma di "espropriazione" di dati è circondata da molte cautele (art. 15)[65], ma rappresenta senz'altro il primo punto di rottura di quel muro eretto a difesa dei

urbana, l'illuminazione pubblica, e dell'ambiente circostante per migliorarne vivibilità, sostenibilità e competitività), di *smart home* (cioè di soluzioni per la gestione in automatico e/o da remoto degli impianti e degli oggetti connessi dell'abitazione, al fine di ridurre i consumi energetici e migliorare il comfort, la sicurezza dell'abitazione e delle persone), di *smart metering* (cioè di contatori connessi per la misurazione dei consumi di elettricità, gas, acqua, calore, e per la loro corretta fatturazione e telegestione), e di *smart factory* (cioè la connessione dei macchinari, degli operatori e dei prodotti per attivare nuove logiche di gestione della produzione); cfr. Osservatorio Big Data Analytics & Business Intelligence del Politecnico di Milano.

59. Ai sensi dell'art. 2, par. 1, n. 15) sono "dati del prodotto": «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».
60. Ai sensi dell'art. 2, par. 1, n. 16) sono "dati di un servizio correlato": «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. Ai sensi dell'art. 5, par. 1: «su richiesta di un utente, o di una parte che agisce per conto di un utente, il titolare dei dati mette a disposizione di terzi i dati prontamente disponibili, nonché i pertinenti metadati necessari a interpretare e utilizzare tali dati, senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo continuo e in tempo reale».
62. Ai sensi dell'art. 2, par. 1, n. 12) è definito "titolare dei dati": «una 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».
63. Ai sensi dell'art. 2, par. 1, n. 13) è definito "destinatario dei dati": «una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione».
64. Norma che trova un suo precedente nell'art. 19 da legge francese *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique* che ha introdotto l'art. 3-*bis* della *Loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques*, a norma del quale è consentito al settore pubblico di accedere a determinati dati del settore privato per finalità di rilevazioni statistiche obbligatorie.
65. Articolo 15 (*Necessità eccezionale di utilizzare i dati*): «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

dataset delle grandi piattaforme digitali, spesso proprio grazie alla normativa in materia di *data protection*, e che costituisce tutt'oggi la principale barriera all'ingresso nei mercati digitali (in questo senso, le recenti vicende in materia di divieto di *web scraping* altro non fanno che consolidare il dominio esclusivo delle Big Tech sui dati generati dagli utenti[66]).

3.5. La Proposta di *Financial Data Access Act*

La medesima logica di accessibilità e condivisione dei dati si affaccia, naturalmente, anche nel settore finanziario, nel quale la Commissione europea ha avanzato una proposta di regolamento che mira a disciplinare l'accesso ai dati dei clienti e il relativo utilizzo. L'accesso ai dati finanziari si riferisce all'accesso ai dati e al loro trattamento sia da parte del cliente verso l'impresa, sia – ed è il profilo più delicato – tra imprese.

La proposta muove dalla considerazione per cui «l'*economia dei dati finanziari* dell'Unione» è frammentata, caratterizzata da «*disomogeneità nella condivisione dei dati*, ostacoli e una forte riluttanza dei portatori di interessi a condividere dati al di là dei conti di pagamento». Per conseguenza «*i clienti non beneficiano di prodotti e servizi personalizzati* basati sui dati in grado di soddisfare le loro esigenze specifiche». L'assenza di prodotti finanziari personalizzati «*limita le possibilità di innovazione*, offrendo una scelta più ampia e maggiori prodotti e servizi finanziari ai consumatori interessati che potrebbero altrimenti beneficiare di *strumenti basati sui dati* che li aiutino a compiere scelte informate, a confrontare facilmente le offerte e a passare a prodotti più vantaggiosi che *corrispondano alle loro preferenze sulla base dei loro dati*»[67].

La proposta abbraccia la quasi totalità dei dati dei clienti raccolti o prodotti da enti finanziari[68] nell'ambito dei servizi finanziari[69], ivi incluso il delicatissimo profilo della valutazione del merito di credito, e prevede una serie di

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».

66. Si veda in particolare l'avvio dell'Indagine conoscitiva sul *web scraping* per l'addestramento degli algoritmi di intelligenza artificiale da parte del Garante. Cfr. anche Garante per la protezione dei dati personali, Provvedimento del 17 maggio 2023, n. 201.
67. Considerando n. 6.
68. Ai sensi dell'art. 2, par. 2, della proposta sono "enti finanziari": «a) enti creditizi; b) istituti di pagamento […]; c) istituti di moneta elettronica […]; d) imprese di investimento; e) prestatori di servizi per le cripto-attività; f) emittenti di token collegati ad attività; g) gestori di fondi di investimento alternativi; h) società di gestione di organismi d'investimento collettivo in valori mobiliari; i)imprese di assicurazione e di riassicurazione; j) intermediari assicurativi e intermediari assicurativi a titolo accessorio; k) enti pensionistici aziendali o professionali; l) agenzie di rating del credito; m) fornitori di servizi di crowdfunding; n) fornitori di PEPP; o) prestatori di servizi di informazione finanziaria».
69. Ai sensi dell'art. 2, par. 1, della proposta, i dati dei clienti soggetti all'applicazione del regolamento fanno riferimento a: «a) contratti di credito ipotecario, prestiti e conti […]; b) risparmi, investimenti in strumenti finanziari,

diritti e obblighi in capo a "titolari dei dati"[70] e "utenti dei dati"[71].

In particolare, per quanto qui interessa, l'art. 5 della proposta disciplina l'obbligo per il titolare dei dati di mettere i dati del cliente a disposizione di un terzo (definito, con una formula non felicissima, utente dei dati) a cui lo stesso cliente ha concesso l'autorizzazione all'accesso ai propri dati. Tale messa a disposizione deve avvenire «senza indebito ritardo, in maniera continuativa e in tempo reale».

In sostanza, un *promoter* finanziario che ottenga da una persona, fisica o giuridica, l'autorizzazione ad accedere, ad esempio, ai dati bancari, potrà presentarsi presso la sua banca e ottenere – in qualità di utente dei dati – tutte le informazioni utili a strutturare un prodotto finanziario personalizzato da sottoporgli. I rischi derivanti da potenziali pratiche ingannevoli o aggressive sono arginati da alcune misure (la cui efficacia sarà certamente da verificare) previste dalla normativa: innanzitutto la predisposizione di un "pannello di gestione delle autorizzazioni" a disposizione del cliente nel quale siano elencate tutte le autorizzazioni in essere (art. 8), e poi la configurazione di "sistemi di condivisione di dati finanziari" notificati e vigilati da un'autorità indipendente (artt. 9 ss.).

4. I dati come beni non rivali nella teoria dei beni comuni

La rassegna normativa sin qui svolta mostra abbastanza chiaramente che i dati, personali e non personali, sono destinati ad una sempre maggiore circolazione e che la legislazione europea non rallenta affatto, anzi incoraggia fortemente, questo fenomeno. Non solo. Il processo di allontanamento dal modello proprietario di controllo sui dati (se non di vero e proprio abbandono), di cui si diceva in apertura, conduce a trattare sempre più i dati come "risorse comuni", condivise tra più soggetti. Sullo stesso set di dati potranno coesistere numerose situazioni giuridiche soggettive diverse, ciascuna delle quali foriera di specifici diritti, obblighi, oneri.

La domanda che dunque occorre porsi è: "di chi saranno i dati?". Di coloro ai quali si riferiscono? Di chi li riceve? Di chi li acquista? Di chi li usa? Di chi sa ricavare da essi un valore? Il quesito non è di ordine meramente teorico, ma anzi – come si dirà tra un attimo – dalla risposta a questa domanda possono derivare conseguenze significative sul piano giuridico.

La natura "non rivale" dei dati (questa, sì, certa) potrebbe consentire di rispondere che tutti questi soggetti potranno contemporaneamente vantare un autonomo, non parziario, titolo giuridico sugli stessi dati. Senza indulgere eccessivamente in questioni su cui si è già espressa attenta dottrina[72], può osservarsi come il "valore" che sino ad oggi abbiamo riconosciuto ai dati (principalmente quali corrispettivo di servizi) è destinato ad accrescersi proprio grazie alle successive possibilità di sfruttamento, derivanti dalla condivisione e dall'accesso di terze parti. Con la conseguenza che non soltanto la governance dei dati si caratterizzerà per una dimensione sempre più collettiva[73], ma la natura stessa dei dati è destinata a cambiare: da oggetti di diritti esclusivi a oggetti di diritti collettivi.

Del resto, per quanto recenti accadimenti abbiano confermato che i dati sono *funzionalmente*

prodotti di investimento assicurativi, cripto-attività, beni immobili e altre attività finanziarie correlate, nonché i benefici economici derivanti da tali attività […]; c) diritti pensionistici negli schemi pensionistici aziendali o professionali […]; d) diritti pensionistici sulla fornitura di prodotti pensionistici individuali paneuropei […]; e) prodotti di assicurazione non vita […]; f) dati che fanno parte di una valutazione del merito creditizio di un'impresa, raccolti nell'ambito di una procedura di richiesta di prestito o di una richiesta di rating del credito».

70. Ai sensi dell'art. 3, par. 1, n. 5), il "titolare dei dati" è definito come: «un ente finanziario diverso da un prestatore di servizi di informazione sui conti che raccoglie, conserva e altrimenti tratta i dati di cui all'articolo 2, paragrafo 1».

71. Ai sensi dell'art. 3, par. 1, n. 6), l'"utente dei dati" è definito come: «una delle entità di cui all'articolo 2, paragrafo 2, che, previa autorizzazione di un cliente, ha accesso legittimo ai dati del cliente di cui all'articolo 2, paragrafo 1».

72. Versaci 2022, p. 13 ss., laddove evidenzia le incongruenze dell'applicazione di un paradigma strettamente proprietario al regime giuridico dei dati, in particolare non personali.

73. Resta 2022, p. 971 ss.; cfr. anche Iannuzzi 2021, p. 31 ss.; Bravo 2021, p. 199 ss.

utilizzati al posto del denaro (sia dalle grandi piattaforme che dai singoli utenti)[74], i dati non sono – *strutturalmente* – beni comparabili al denaro. Il fenomeno di *impoverimento-arricchimento* che si verifica in una transazione basata su valori monetari, non si realizza laddove la controprestazione di una obbligazione sia costituita da dati: il consumatore "paga", ma non si impoverisce. I dati che lo riguardano continuano ad essere *anche* suoi.

Queste forme di "compossesso"[75], dunque, unite alle proporzioni di larga scala assunte dai *big data* collazionati dai grandi *player* economici globali, inducono a considerare seriamente una loro qualificazione alla stregua di "beni comuni" (*commons*)[76].

Sebbene non esista un univoco concetto giuridico di beni comuni[77], questa categorizzazione può risultare utile non solo al fine di definire lo statuto giuridico dei dati all'indomani di questa imponente ondata regolatoria europea, ma altresì a giustificare le sempre maggiori istanze di accesso e condivisione dei dati, specie nel flusso che va dal settore privato a quello pubblico.

Andiamo con ordine e muoviamo anzitutto dalla prospettiva economica: i beni comuni sono tradizionalmente considerati "rivali" e "non escludibili"[78], ragion per cui si verifica quella che Garret Hardin chiamava la "tragedy of commons": tutti coloro che concorrono allo sfruttamento della risorsa sono anche coloro che ne determinano l'esaurimento[79]. L'unico modo per evitarlo viene così da questi individuato nella proprietà pubblica, che sottrae i beni alla appropriazione individuale. Teorie successive hanno però superato la dicotomia tra privato e pubblico, accedendo a forme intermedie di governo collettivo dei beni comuni. È questa in particolare l'impostazione propria di Elinor Ostrom[80], premio Nobel per l'economia del 2009, la quale ha dimostrato come assetti "istituzionali", non pubblici, nel governo dei beni collettivi siano in grado di assicurare nel tempo la *sostenibilità* dello sfruttamento della risorsa collettiva, di fatto riconoscendo lo spazio per una terza via, tra stato e mercato, tra pubblico e privato[81].

Ebbene, tornando al nostro campo d'indagine, i dati sono la risorsa collettiva globale del nostro tempo (per giunta non rivale, dunque inesauribile), il cui governo è a tutt'oggi in mano a pochi, enormi, poteri privati[82], che esercitano su di essi un controllo di fatto esclusivo ed escludente. I dati, infatti, dal momento in cui sono "rilasciati" dall'interessato al titolare del trattamento, si inseriscono in circuiti economici di larghissima scala a tutto vantaggio delle *Big Tech*, mentre gli utenti si limitano a beneficiare di qualche servizio gratuito.

Considerare quindi i dati (specie quelli personali e quelli che derivano dai dati personali a séguito di procedimenti di anonimizzazione) come "beni comuni"[83] avrebbe il pregio di riconoscere la provenienza *collettiva* e *relazionale* di tale fonte di

74. V. *supra*, nota 3.

75. Che riecheggiano forme di proprietà collettiva antecedenti all'avvento dello stato liberale e del diritto di proprietà come diritto assoluto. Cfr. Grossi 1977, *passim*.

76. Cfr. sul tema Fia 2021, p. 185 ss.

77. Si veda Cerulli Irelli-De Lucia 2014, p. 6 ss., laddove rilevano almeno 4 accezioni diverse: i) interessi e valori generali, di tono costituzionale; ii) beni immateriali di importanza centrale per la società; iii) cose in senso giuridico strumentali all'esercizio di diritti fondamentali della persona; iv) spazi fisici goduti da una collettività. Cfr. anche Marella 2012, p. 18; Hess-Ostrom 2003, p. 114 ss.; in generale sul tema, si veda: Arena 2022, p. 647 ss; Cerulli Irelli 2022, p. 639 ss.; Ciervo 2012; Rodotà 2013, p. 105.

78. Brosio 2021, pp. 32-34.

79. Hardin 1968, p. 162 ss.

80. In particolare, Ostrom 1990.

81. Cfr. anche Ostrom-Schroeder-Wynne 1993.

82. Sia consentito rinviare a Cremona 2023. Cfr. Ferrarese 2022, p. 138. Betzu 2020. O ancora l'intero fascicolo n. 3/2021 della rivista *Diritto Pubblico* dedicato ai poteri privati, del quale si richiamano qui – sul tema Big Tech – i contributi di Betzu 2021; Brandimarte-Pecchi-Piga 2021; Di Gaspare 2021; Ferrarese 2021; Libertini 2021; Pardolesi 2021.

83. Cfr. Nissenbaum 2009; Sanfilippo-Frischmann-Standburg 2018; Wong-Henderson-Ball 2022; Mills 2019.

ricchezza e dunque di giustificare anche politiche "restitutorie", come quella della ridetta "espropriazione" dei dati per necessità eccezionali (*ex* art. 14 del *Data Act*) o dell'accesso pubblico ai dati detenuti dai privati per finalità di beneficio comune.

5. *Data for Good*: prospettive di *data sharing* per le imprese nel quadro della regolamentazione di sostenibilità

Iniziare a considerare – a certi fini e a certe condizioni – i dati in possesso delle imprese (o almeno quelli delle grandi piattaforme digitali) come beni comuni può creare le premesse per interventi normativi che restituiscano agli utenti, sia pure indirettamente, una parte della ricchezza generata proprio a partire dai dati loro riferibili. Le petizioni in questo senso sono molte e crescenti[84].

Non è difficile immaginare l'ampiezza dei settori nei quali i dati in mano a soggetti privati potrebbero risultare utili per il bene comune[85]: si pensi banalmente ai dati sul traffico e in generale sugli spostamenti, con significativi potenziali impatti diretti sull'ambiente, ai dati sull'istruzione, sull'accesso al lavoro, a quelli sulla salute ricavati dagli *wearables*, e a tutte le informazioni che sarebbero preziose nella definizione di politiche pubbliche e nell'erogazione dei servizi pubblici[86].

Secondo recenti rilevazioni, l'accesso degli enti pubblici (in particolare delle amministrazioni locali[87]) ai dati del settore privato di interesse pubblico è ancora una pratica emergente e sporadica[88]. Alcuni report riferiscono di una percepita asimmetria di potere (a vantaggio del settore privato) nella condivisione dei dati verso le amministrazioni locali, non esistendo ad oggi ancora strumenti giuridici vincolanti per l'accesso a tali informazioni. Solo si danno alcune virtuose esperienze volontarie di c.d. *data philantropy*[89].

Vi sono però, anche in una prospettiva *de jure condito*, strumenti giuridici che potrebbero essere valorizzati al fine di promuovere la condivisione *stabile* di dati dal settore privato a quello pubblico. Il riferimento è al *framework* normativo cosiddetto ESG (*environmental*, *social*, *governance*) e in particolare alla Direttiva europea in materia di *Corporate Sustainability Reporting* (c.d. CSRD)[90], entrata

84. Si veda già Mazzuccato 2018, ove afferma: «Let's not forget that a large part of the technology and necessary data was created by all of us, and should thus belong to all of us. The underlying infrastructure that all these companies rely on was created collectively (via the tax dollars that built the internet), and it also feeds off network effects that are produced collectively. There is indeed no reason why the public's data should not be owned by a public repository that sells the data to the tech giants, rather than vice versa. But the key issue here is not just sending a portion of the profits from data back to citizens but also allowing them to shape the digital economy in a way that satisfies public needs. Using big data and AI to improve the services provided by the welfare state – from health care to social housing – is just one example».

85. Alemanno 2018; OECD 2015; Farmer-McCosker-Albury-Aryani 2023.

86. Si vedano in questa direzione le iniziative, ad esempio, del *Data for Road Safety* o dei *Data Collaboratives*. Cfr. Commissione europea 2020.

87. Cfr. Giannelli-Pagnanelli 2023; Vigorito 2023, p. 697 ss.; Hardinges 2019.

88. Micheli 2022. L'articolo riporta i risultati di una ricerca che ha esaminato la condivisione dei dati B2G nelle amministrazioni locali europee. Basandosi su interviste con responsabili di progetto di dodici comuni, lo studio ha contestualizzato l'accesso ai dati del settore privato nella prospettiva di coloro che lavorano nel settore pubblico.

89. McKeever-Greene-MacDonald-Tatian 2018.

90. La CSRD UE 2022/2464 (pubblicata nella Gazzetta Ufficiale UE il 16 dicembre 2022) modifica la normativa europea emendando la Direttiva 2004/109/CE sull'armonizzazione degli obblighi di trasparenza riguardanti le informazioni sugli emittenti i cui valori mobiliari sono ammessi alla negoziazione in un mercato regolamentato; la Direttiva 2006/43/CE relativa alle revisioni legali dei conti annuali e dei conti consolidati; le Direttive 2013/34/UE e 2014/95/UE relative ai bilanci d'esercizio, ai bilanci consolidati, alle relative relazioni di talune tipologie e alla comunicazione di informazioni di carattere non finanziario e di informazioni sulla diversità da parte di talune imprese e di taluni gruppi di grandi dimensioni; il Regolamento UE 537/2014 sui requisiti specifici relativi alla revisione legale dei conti di enti di interesse pubblico. Cfr. in tema Genovese 2023, p. 88 ss.; Fortunato 2019, p. 420 ss.

in vigore il 5 gennaio 2023, in forza della quale le imprese ricadenti nell'ambito soggettivo di applicazione della direttiva[91] saranno tenute a comunicare al pubblico "informazioni sulla sostenibilità" che, come è noto, si declina nei fattori ambientali, sociali e di governo dell'impresa. A questa si affianca la Proposta di *Corporate Sustainability Due Diligence Directive* (CSDDD)[92], che, in omaggio a un dichiarato *stakeholderism*, integra i doveri di diligenza dell'impresa nei confronti di tutti i portatori di interesse[93].

Ebbene, se gli obblighi positivi in campo ambientale e di governance sono forse più chiari e normati, quelli in campo sociale sono, a detta dei più, ancora sfuggenti e non chiaramente definiti. Sotto questo profilo, l'adozione di policy di *data sharing* rappresenta per le imprese una opportunità non soltanto per concorrere a finalità di beneficio comune, ma altresì di compliance ad un plesso normativo – quello sulla sostenibilità – sempre più rilevante e penetrante.

Riferimenti bibliografici

A. Alemanno (2018), *Data for good: unlocking privately held data to the benefit of the many*, in "European Journal of Risk Regulation", vol. 9, 2018, n. 2

G. Arena (2022), *Da beni pubblici a beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

K. Ashton (2009), *That 'Internet of Things' Thing*, in "rfidjournal.com", 22 June 2009

V. Bachelet (2023), *La Corte di giustizia sul caso Meta: trattamento di dati e "prezzo" del consenso*, in "Pactum", 2023, n. 4

M. Betzu (2021), *I poteri privati nella società digitale: oligopoli e antitrust*, in "Diritto pubblico", 2021, n. 3

M. Betzu (2020), *Poteri pubblici e poteri privati nel mondo digitale*, in P. Costanzo, P. Magarò, L. Trucco (a cura di), "Il diritto costituzionale e le sfide dell'innovazione tecnologica", 2020

L. Brandimarte, L. Pecchi, G. Piga (2021), *Le imprese Big Tech: schiave delle leggi per poter essere liberi?*, in "Diritto pubblico", 2021, n. 3

F. Bravo (2021), *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in "Contratto e impresa Europa", 2021, n. 1

C. Brescia Morra (2022), *Chi salverà il mondo? Lo stato o le grandi corporations? ESG: una formula ambigua e inutile*, in "Rivista trimestrale di diritto dell'economia", 2022, n. 4

G. Brosio (2021), *Economia pubblica moderna*, Giappichelli, 2021

91. La direttiva riguarda: i) grandi imprese non quotate che alla data della chiusura del bilancio, anche su base consolidata, abbiano superato almeno due dei seguenti criteri dimensionali: 250 numero medio di dipendenti; € 20 milioni di stato patrimoniale; € 40 milioni di ricavi netti; ii) piccole e medie imprese quotate (escluse le micro-imprese). Sono, inoltre, compresi gli istituti di credito di piccole dimensioni non complessi e le imprese di assicurazioni dipendenti da un Gruppo; iii) imprese e figlie di succursali con capogruppo extra-UE per le quali la capogruppo abbia generato in UE ricavi netti superiori a € 150 milioni per ciascuno degli ultimi due esercizi consecutivi e almeno: un'impresa figlia soddisfi i requisiti dimensionali della CSRD; una succursale abbia generato ricavi netti superiori a € 40 milioni nell'esercizio precedente.

92. Commissione europea, Proposta della Commissione di Direttiva del Parlamento europeo e del Consiglio relativa al dovere di diligenza delle imprese ai fini della sostenibilità e che modifica la Direttiva (UE) 2019/1937, COM/2022/71, del 23 febbraio 2022. In tema cfr. Racugno-Scano 2022, p. 726 ss.; Ventoruzzo 2021, p. 386 ss.; nonché l'intero fascicolo 1/2022 della rivista *Analisi Giuridica dell'Economia*, con commenti, tra gli altri di Tombari, Strambelli, Rescigno.

93. Tra i commenti più scettici, Brescia Morra 2022, p. 78 ss.

V. Cerulli Irelli (2022), *Proprietà, beni pubblici, beni comuni*, in "Rivista trimestrale di diritto pubblico", 2022, n. 3

V. Cerulli Irelli, L. De Lucia (2014), *Beni comuni e diritti collettivi*, in "Politica del diritto", 2014, n. 1

A. Ciervo (2012), *I beni comuni*, Ediesse, 2012

Commissione europea (2020), *GDPR – A fabric of a success story*, June 2020

Commissione europea (2020), *Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing*, 2020

Commissione europea (2019), *SME panel consultation - B2B Data Sharing*, October 2019

E. Cremona (2023), *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, ESI, 2023

A. Davola (2021), *"I vestiti nuovi dell'imperatore": il contenzioso tra il Bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in "Diritto di internet", 2021, n. 1

A. De Franceschi, M. Lehmann (2015), *Data As Tradable Commodity and New Measures for Their Protection*, in "The Italian Law Journal", vol. 1, 2015, n. 1

G. De Gregorio, F. Paolucci (2022), *Dati e intelligenza artificiale all'intersezione tra mercato e democrazia*, in E. Cremona, F. Laviola, V. Pagnanelli, "Il valore economico dei dati personali tra diritto pubblico e diritto privato", Giappichelli, 2022

G. Di Gaspare (2021), *Poteri privati e Corporation nella globalizzazione*, in "Diritto pubblico", 2021, n. 3

European Data Protection Supervisor (2020), *Opinion 3/2020, Opinion on the European strategy for data*, 16 June 2020

J. Farmer, A. McCosker, K. Albury, A. Aryani (2023), *Data for social good. Non-Profit Sector Data Projects*, Palgrave Macmillan, 2023

M.R. Ferrarese (2022), *Poteri nuovi. Privati, penetranti, opachi*, il Mulino, 2022

M.R. Ferrarese (2021), *Privatizzazioni, poteri invisibili e infrastrutture giuridiche globali*, in "Diritto pubblico", 2021, n. 3

T. Fia (2021), *An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons*, in "Global Jurist", 2021

S. Fortunato (2019), *L'informazione non-finanziaria nell'impresa socialmente responsabile*, in "Giurisprudenza commerciale", 2019, n. 3

A. Galiano, A. Leogrande, S.F. Massari, A. Massaro (2020), *I dati non personali: la natura e il valore*, in "Rivista italiana di informatica e diritto", 2020, n. 1

A. Genovese (2023), *L'armonizzazione del reporting di sostenibilità delle imprese azionarie europee dopo la CSRD*, in "Contratto e impresa", 2023

M. Giannelli, V. Pagnanelli (2023), *Smart cities*, Giappichelli, 2023

I. Graef (2016), *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Kluwer Law International, 2016

P. Grossi (1977), *Un altro modo di possedere*, Giuffrè, 1977

G. Hardin (1968), *The tragedy of the Commons*, in "Science", 1968

J. Hardinges (2019), *Do cities have access to the private sector data they need to make effective decisions?*, Open Data Institute, 23 July 2019

C. Hess, E. Ostrom (2003), *Ideas, Artifacts, and Facilities: Information as a Common-Pool Resource*, in "Law & Contemporary Problems", 2003

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. Libertini (2021), *Sugli strumenti giuridici di controllo del potere economico*, in "Diritto pubblico", 2021, n. 3

M.R. Marella (a cura di) (2012), *Per un diritto dei beni comuni. Oltre il pubblico e il privato*, Ombre Corte, 2012

M. Mazzuccato (2018), *Let's make private data into a public good*, in "MIT Technology Review", 27 June 2018

B. McKeever, S. Greene, G. MacDonald, P. Tatian (2018), *Data Philanthropy. Unlocking the Power of Private Data for Public Good*, in "Urban Institute", 24 July 2018

M. Micheli (2022), *Public bodies' access to private sector data: The perspectives of twelve European local administrations*, in "First Monday", vol. 27, 2022, n. 2

S. Mills (2019), *Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership*, 24 September 2019

H. Nissenbaum (2009), *Privacy in context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009

OECD (2015), *Data-driven innovation: big data for growth and well-being*, 2015

E. Ostrom (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge University Press, 1990 (trad.it.: *Governare i beni collettivi*, Marsilio, 2006)

E. Ostrom, L. Schroeder, S. Wynne (1993), *Institutional Incentives and Sustainable Development: Infrastructure Policies in Perspective*, Oxford, Westview Press, 1993

R. Pardolesi (2021), *Piattaforme digitali, poteri privati e concorrenza*, in "Diritto pubblico", 2021, n. 3

R. Pardolesi, R. Van den Bergh, F. Weber (2020), *Facebook e i peccati da «Konditionenmissbrauch»*, in "Mercato, concorrenza e regole", 2020, n. 3

K. Pistor (2019), *The Code of Capital. How the Law Creates Wealth and Inequality*, Princeton University Press, 2019

G. Racugno, D. Scano (2022), *Il dovere di diligenza delle imprese ai fini della sostenibilità: verso un Green Deal europeo*, in "Rivista delle società", 2022, n. 4

G. Resta (2022), *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

S. Rodotà (2013), *Mondo delle persone, mondo dei beni*, in Id., "Il diritto di avere diritti", Laterza, 2013

A. Sandulli (2021), *Il diritto quale infrastruttura per i poteri privati? A proposito di un libro di Katharina Pistor*, in "Diritto Pubblico", 2021, n. 3

M. Sanfilippo, B. Frischmann, K. Standburg (2018), *Privacy as Commons: Case Evaluation Through the Governing Knowledge Commons Framework*, in "Journal of Information Policy", vol. 8, 2018

M. Ventoruzzo (2021), *Note minime sulla responsabilità civile nel progetto di direttiva Due Diligence*, in "Rivista delle società", 2021, n. 2-3

G. Versaci (2022), *Note minime sulla circolazione dei dati nei rapporti tra imprese*, in "Studi e materiali. Rivista semestrale del Consiglio nazionale del notariato", 2022, n. 1

A. Vigorito (2023), *Government Access to Privately-Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models*, in G. Resta, V. Zeno-Zencovich (eds.), "Governance of/through Big Data", RomaTrE-Press, 2023

S.D. Warren, L. Brandeis (1890), *The Right to Privacy*, in "Harvard Law Review", IV (5), 1890

J. Wong, T. Henderson, K. Ball (2022), *Data Protection for the common good: Developing a framework for a data-protection-focused data commons*, in "Data & Policy", 2022, n. 4, e3

H. Zech (2015), *Information as Property*, in "Journal of Intellectual Property, Information Technology and E-Commerce Law", vol. 6, 2015, n. 3