



CONSULTA ONLINE

PERIODICO TELEMATICO ISSN 1971-9892



2023 FASC. III

(ESTRATTO)

VALENTINA PAGNANELLI

**PROSPETTIVE SULLA VALORIZZAZIONE DEI DATI PERSONALI
IN AMBITO PUBBLICO**

5 DICEMBRE 2023

IDEATORE E DIRETTORE RESPONSABILE: PROF. PASQUALE COSTANZO

Valentina Pagnanelli
Prospettive sulla valorizzazione dei dati personali in ambito pubblico*

ABSTRACT: *The paper delves into the economic value of personal data, focusing not on the private sector dominated by Big Digital Companies but on the public sector. In this context, the term "valorization" of data is considered more suitable than "monetization." The discussion includes two examples of personal data use in the public sector and references recent European regulatory developments on data governance, including the emergence of data altruism. The aim is to assess how public entities can leverage the informational value of personal data while upholding the fundamental rights and freedoms of individuals.*

SOMMARIO: 1. Patrimonializzazione o valorizzazione dei dati personali? Una riflessione introduttiva. – 2. L’ambivalenza dell’utilizzo dei dati personali in ambito pubblico. – 3. Il *social scoring*. – 4. Il supporto alla elaborazione delle politiche pubbliche. – 4.1 Il *Data Governance Act* e la novità dell’altruismo dei dati. – 4.2 Uno sguardo al futuro: il *Data Act*. – 5. Conclusioni.

1. *Patrimonializzazione o valorizzazione dei dati personali? Una riflessione introduttiva*

La società nella quale tutti noi viviamo, lavoriamo, creiamo relazioni, ci accostiamo alla cultura, curiamo il nostro benessere, è oramai datificata¹. Tutte le attività della vita lasciano una traccia digitale più o meno visibile e “calcolabile”. Non si può negare che l’utilizzo dei dati, da parte di diversi soggetti, e per le più svariate finalità, abbia degli effetti giuridici, sociali, e certamente anche economici².

Per essere più chiari basterà fare qualche esempio: molte delle applicazioni che offrono gratuitamente dei servizi da installare nei dispositivi mobili ci chiedono in cambio l’autorizzazione a trattare i nostri dati personali: i grandi motori di ricerca e i *social network* che ci permettono di navigare, cercare informazioni, creare pagine personali, intessere relazioni virtuali, costruiscono il loro modello di *business* sulla elaborazione dei nostri dati personali e la conseguente vendita di spazi pubblicitari altamente profilati³; gli istituti di credito pongono l’utilizzo di strumenti di *fintech* alla base delle loro decisioni di prestito⁴. Gli esempi potrebbero proseguire, toccando molti altri settori e fattispecie e coinvolgendo in modo profondo i diritti e le libertà delle persone e i principi democratici⁵.

In questa sede non potremo fare che qualche cenno a questioni che meriterebbero bel altro approfondimento e delimitaremo il campo di indagine, ragionando sulla configurabilità della valutazione economica dei dati personali nel settore pubblico. Infatti, se è pur vero che, anche intuitivamente, si possa comprendere che nelle attività che si svolgono nel settore privato i dati possano essere utilizzati per estrarne valore economico (resta comunque da comprendere quali siano gli schemi giuridici più adatti per legittimare determinate attività e al contempo tutelare i diritti



¹ *Ex plurimis*, L. FLORIDI, *La quarta rivoluzione. Come l’infosfera sta trasformando il mondo*, Raffaello Cortina Editore, Milano, 2017; S. CALZOLAIO, *Protezione dei dati personali, aggiornamento*, in *Digesto delle discipline pubblicistiche*, Utet, Torino, 2017, 598; F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell’era digitale*, Giuffrè Francis Lefebvre, Milano, 2019.

² Per una panoramica sul tema, sia consentito rinviare al volume E. Cremona, F. Laviola. V. Pagnanelli (a cura di), *Il valore economico dei dati tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022.

³ Cfr. V. PAGNANELLI, *Una “valutazione d’impatto” della privacy sulle Big Tech. Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. Cremona, F. Laviola. V. Pagnanelli (a cura di), *Il valore economico dei dati*, cit., 13.

⁴ «Le banche si affidano ai “punteggi di credito” (*credit scoring*) per prendere decisioni sui prestiti alle imprese e ai clienti persone fisiche, utilizzando come base dati, non solo le transazioni e le “storie” di pagamento dei clienti, ma anche fonti di dati aggiuntive (i c.d. “dati alternativi”), come l’attività sui social media, l’uso dello smartphone, l’attività dei messaggi di testo», cfr. F. BAGNI, *Il consumatore “prevedibile”: Big Data e intelligenza artificiale nella erogazione dei servizi bancari*, in E. Cremona, F. Laviola. V. Pagnanelli (a cura di), *Il valore economico dei dati*, cit., 78-79.

⁵ Per tutti, S. ZUBOFF, *Il capitalismo della sorveglianza: il futuro dell’umanità nell’era dei nuovi poteri*, Luiss University Press, Roma, 2019.

fondamentali delle persone fisiche), ben diverso è lo scenario quando ci si pongano le medesime domande in relazione all'utilizzo dei dati in ambito pubblico. Proveremo, dunque, a riflettere su alcuni aspetti del trattamento dei dati nel settore pubblico ed in particolare sulle modalità della loro patrimonializzazione.

Prima di procedere appare necessario chiarire che, in tutto quanto attiene allo svolgimento di attività a beneficio della collettività, il profilo della economicità potrà emergere più agevolmente solo in relazione ad una valutazione economica dei risultati di determinate politiche pubbliche e scelte di governo (sia locale, sia di livello più elevato). Alla luce di queste premesse, si procederà pertanto a svolgere alcune considerazioni che abbiano ad oggetto l'utilizzo e quella che più propriamente si potrebbe definire la *valorizzazione* (in senso lato) dei dati nel settore pubblico, tralasciando l'aspetto più strettamente connesso alla monetizzazione dei dati personali. Dunque, si procederà prendendo ad esempio due tipologie di trattamento di dati personali nel settore pubblico, evidenziandone alcune peculiarità e potenzialità, anche alla luce della produzione normativa dell'Unione europea.

2. L'ambivalenza dell'utilizzo dei dati personali in ambito pubblico

La comparsa sulla scena e l'esponentiale sviluppo di sistemi di Intelligenza Artificiale hanno esteso in pochissimi anni il potenziale dei *Big Data*⁶, accrescendo l'elenco dei possibili utilizzi di questa tecnologia innovativa.

Se, da un lato, i risultati della ricerca appaiono prodromici al miglioramento della vita dei cittadini, ai grandi progressi della scienza, alla soluzione della crisi climatica, alla lotta alla criminalità, dall'altro, gli stessi strumenti potrebbero, se utilizzati in modo malevolo, provocare danni gravissimi e perdita dei diritti degli individui. Se si prende come scenario di riferimento il settore pubblico, dimora dei poteri dello Stato e della tutela delle garanzie costituzionali, il confine tra la valorizzazione dei dati per il bene pubblico e le pericolose derive di un utilizzo distorto (discriminazioni, sorveglianza ubiqua, disinformazione, turbative alla democrazia) diviene sottile e grave sarebbe un suo superamento.

I due casi di studio su cui ci soffermeremo tra poco vorrebbero contribuire ad evidenziare alcune di queste delicate questioni. Essi riguardano l'utilizzo (e la valorizzazione) dei dati per diverse finalità: l'incoraggiamento ad una cittadinanza "virtuosa", attuato attraverso meccanismi di raccolta dei dati ed elaborazione di punteggi (che, nella loro realizzazione concreta, potrebbero servire ad incoraggiare la buona cittadinanza o al contrario a controllare in modo pervasivo i cittadini) e l'elaborazione delle politiche a favore dei cittadini ed il miglioramento nella progettazione e realizzazione dei servizi.

3. Il social scoring

Per quanto riguarda il primo caso, cioè il *social scoring*, il Regolamento europeo 2016/679 (GDPR)⁷ prevede una tutela per le persone fisiche. Si tratta in realtà di un divieto esplicito per il

⁶ Sui *Big Data*, *ex plurimis*, M. DELMATRO, A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, il Mulino, Bologna, 2019; R. KITCHIN, G. MCARDLE, *What makes Big Data, Big Data?*, in *Big Data & Society*, 2016; G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e Big Data*, in E. Tosi (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Giuffrè Francis Lefebvre, Milano, 2019, 447 ss.; S. FARO, N. LETTIERI, *Big Data: una lettura informatico-giuridica*, in *Scritti per Luigi Lombardi Vallauri*, Cedam, Padova, 2016, I, 503 ss.

⁷ [Regolamento \(UE\) 2016/679 del Parlamento 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 \(Regolamento generale sulla protezione dei dati\)](#). V. G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, La

titolare del trattamento, cioè per il soggetto che ha la responsabilità di individuare finalità e mezzi del trattamento dei dati personali, di sottoporre l'interessato a decisioni basate unicamente sul trattamento automatizzato dei dati personali.

Tra i trattamenti automatizzati la norma (l'articolo 22 del GDPR⁸) cita esplicitamente la profilazione e specifica che il trattamento non deve produrre effetti giuridici sull'interessato, né deve incidere significativamente sulla sua persona. La formulazione di questa norma sembrerebbe escludere completamente la possibilità di procedere ad una valutazione del credito dei cittadini, anche se al fine di sollecitarli ad una buona cittadinanza.

In realtà, i paragrafi 2 e 3 pongono una serie di eccezioni al divieto che aprono la strada a molte opzioni di utilizzo della valutazione dei cittadini. Per quel che qui interessa, l'art. 6 par. 2 lett. b) prevede che il divieto possa essere superato per legge, ove il diritto dell'Unione o dello Stato membro indichi anche le misure adeguate a tutela dei diritti e delle libertà dell'interessato. Il paragrafo 3 autorizza persino l'utilizzo di categorie particolari di dati alla base del trattamento automatizzato, purché sia svolto per motivi di rilevante interesse pubblico, con misure di tutela adeguate, *ex art.* 9 par. 2 lett. g) del GDPR⁹. La norma introduce l'ipotesi del consenso esplicito dell'interessato (par. 2 lett. c) e par. 3), che pare comunque non applicabile anche in virtù di quanto espresso nel GDPR¹⁰ e della consolidata posizione del Gruppo di lavoro Articolo 29¹¹.

Se, dunque, dal GDPR non sembra giungere una indicazione che in modo netto autorizzi o escluda questo tipo di trattamenti, indicazioni più chiare sembrano giungere dalla proposta di Regolamento europeo sull'Intelligenza Artificiale (*Artificial Intelligence Act*¹²). In essa compare un divieto per le autorità pubbliche di utilizzare meccanismi di *social scoring* con possibili fini discriminatori. L'articolo 5 prevede il divieto di utilizzo di pratiche di intelligenza artificiale ritenute particolarmente rischiose in ragione dell'applicazione di tecniche subliminali o di sistemi che sfruttino la vulnerabilità di categorie fragili o perché comportino l'identificazione biometrica in tempo reale. Tra le pratiche vietate, compare anche l'utilizzo, da parte delle autorità pubbliche, di sistemi atti a valutare l'affidabilità delle persone «*sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste*», nei casi in cui il punteggio sociale ottenuto sia causa di un trattamento pregiudizievole o sfavorevole, ingiustificato o sproporzionato¹³.

protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101, Zanichelli, Bologna, 2019, 1 ss.

⁸ Tra i commenti all'art. 22 del Regolamento europeo n. 2016/679, *ex plurimis*, F. LAGIOIA, G. SARTOR G., A. SIMONCINI, *Articolo 22*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della Privacy e Data protection*, Milano, 2021, 378 ss.; G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Ipsoa, Milano, 2018, 219 ss.; L. Bolognini L., E. Pelino (a cura di), *Codice della disciplina privacy*, Giuffrè Francis Lefebvre, Milano, 2019, 181 ss.

⁹ V. A. THIENE, *Art. 9*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, cit., 239 ss.

¹⁰ Che al Considerando n. 43 chiarisce che «*Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente [...]*».

¹¹ Cfr. GRUPPO DI LAVORO ARTICOLO 29, [Linee guida sul consenso ai sensi del regolamento \(UE\) 2016/679](#), WP 259 rev.01, 28 novembre 2017, 6.

¹² [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, COM\(2021\) 206 final](#). Si vedano, *ex plurimis*, i commenti di C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla Proposta di Regolamento dell'Unione Europea in materia di Intelligenza Artificiale*, in [Biolaw Journal](#) n. 3/2021, 415 ss.; A. SIMONCINI, *Verso la regolamentazione della Intelligenza Artificiale. Dimensioni e governo*, *ibid.*, 2/ 2021; A. MANTELEO, *Sulle regole AI l'Europa sceglie approccio "industriale": luci e ombre*, in [Agenda Digitale eu](#), 27 aprile 2021. V. anche il volume *La via europea per l'Intelligenza artificiale* (a cura di C. Camardi), Wolters Kluwer Cedam, Milano, 2022.

¹³ V. [Proposta di Regolamento sull'Intelligenza Artificiale](#), art. 5, par. 1 lett. c). Si noti che nell'emendamento 218, adottato dal Parlamento europeo il 14 giugno 2023 scompare il riferimento alle sole autorità pubbliche, e viene eliminato altresì il termine «*affidabilità*», in favore di un più ampio riferimento alla valutazione o classificazione di persone singole o di gruppi di persone tramite *social scoring*, Cfr. PARLAMENTO EUROPEO, [Emendamenti del Parlamento europeo](#),

4. Il supporto alla elaborazione di politiche pubbliche

Per quanto riguarda il secondo profilo, cioè la valorizzazione dei dati ai fini dell'elaborazione di politiche a favore della collettività ed il miglioramento dei servizi pubblici, merita di essere richiamato il più ampio contesto della "Strategia europea per i dati", elaborata e presentata nel febbraio 2020.

L'Unione europea ha, infatti, deciso di imprimere una spinta allo sviluppo del Mercato Unico Digitale attraverso interventi volti ad aumentare la quantità di dati a disposizione delle imprese¹⁴, anche ai fini dell'addestramento dei sistemi di Intelligenza Artificiale¹⁵. L'Unione ha deciso di procedere con l'approvazione di norme, l'individuazione di strumenti idonei, la realizzazione di infrastrutture, la creazione di competenze per la gestione dei dati per favorire l'aumento di dati conservati ed elaborati nell'UE¹⁶ e di realizzare uno spazio unico europeo dei dati affidabile ed attraente per investitori ed imprese. È la Commissione stessa a constatare che mentre l'utilizzo dei dati del settore pubblico da parte delle imprese è ormai da lungo tempo ampiamente garantito da politiche consolidate dell'Unione, i dati del settore privato messi a disposizione del settore pubblico non sono ancora sufficienti affinché possano essere utilizzati e valorizzati in termini di miglioramento delle politiche e dei servizi pubblici¹⁷. Di conseguenza, seppure all'interno di una serie di interventi finalizzati innanzitutto a favorire la libera circolazione dei dati nello spazio giuridico europeo e ad aumentarne il volume a disposizione delle imprese, alcune iniziative legislative della Commissione appaiono mirate a garantire anche agli attori del settore pubblico la disponibilità di dati sufficienti per la predisposizione di politiche *data-driven* a beneficio della collettività.

4.1 Il Data Governance Act e la novità dell'altruismo dei dati

Sul versante dell'apertura dei dati pubblici in favore del settore privato, accanto alla Direttiva 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico¹⁸, si colloca il Regolamento sulla *governance* dei dati (*Data Governance Act - DGA*)¹⁹, di recente approvazione. Il *DGA* stabilisce regole per il riutilizzo, a determinate condizioni, dei dati detenuti da enti pubblici che siano soggetti a diritti di terzi. Si tratta dei dati protetti per motivi di riservatezza commerciale, riservatezza statistica, protezione della proprietà intellettuale, protezione dei dati personali²⁰.

Se è vero che il *Data Governance Act* mira a promuovere la disponibilità dei dati riutilizzabili, potenziando i sistemi di condivisione in tutta l'Unione europea²¹, è indubitabile che lo stesso articolato contiene norme che incentivano i flussi di dati anche *verso* i soggetti pubblici.

[approvati il 14 giugno 2023, alla 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 \(COM\(2021\)0206 – C9-0146/2021 – 2021/0106\(COD\)\).](#)

¹⁴ COMMISSIONE EUROPEA, [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 final, 19 febbraio 2020, 5.

¹⁵ *Ibid.*, 3.

¹⁶ *Ibid.*, 5.

¹⁷ *Ibid.*, 7.

¹⁸ [Direttiva \(UE\) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.](#)

¹⁹ [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 \(Data Governance Act\).](#) Per un commento, v. F. COLAPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in [L post di AISDUE](#), Focus "Servizi e piattaforme digitali", n. 3, 5 maggio 2021.

²⁰ Cfr. [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 \(Data Governance Act\)](#), art. 3.

²¹ V. D. POLETTI, *Gli intermediari dei dati*, in [European Journal of Privacy Law and Technologies](#), 1/2022, 46-48; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 971 ss.

Certamente di rilievo sotto il profilo dell'incremento dei dati a disposizione del settore pubblico ai fini del miglioramento delle politiche e delle attività amministrative, è l'introduzione nel *DGA* di un'ipotesi di utilizzo di dati messi a disposizione dagli interessati su base volontaria, per perseguire obiettivi di interesse generale quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione nella realizzazione di statistiche, il miglioramento delle politiche e dei servizi pubblici, il sostegno alla ricerca scientifica²².

Gli Stati membri dovrebbero predisporre sistemi e strumenti tali da agevolare l'espansione della pratica della donazione dei dati sulla base del consenso informato. A tal fine, l'articolo 25 prevede l'elaborazione di un modello europeo di consenso all'altruismo dei dati che si presenti con un formato uniforme in tutti gli Stati membri²³. Il *Data Governance Act* prevede anche la possibilità di costituire e registrare organizzazioni senza scopo di lucro che svolgano attività di altruismo dei dati, destinatarie di obblighi di trasparenza e di obblighi specifici posti a tutela dei diritti degli interessati e dei titolari dei dati²⁴.

Il nuovo istituto dell'altruismo dei dati ci riconduce alla questione all'origine di questo contributo, ovvero la patrimonializzazione dei dati personali. Un argomento frequentemente utilizzato da coloro che sostengono la non commerciabilità dei dati personali è la riconduzione di tale espressione digitalizzata della personalità alla sfera dei diritti fondamentali, che hanno tra le loro caratteristiche l'indisponibilità e l'inalienabilità. Questione su cui si è incentrata la difesa di *Facebook* nella nota disputa che la vide contrapposta all'Autorità antitrust italiana e che si concluse con [la sentenza del Consiglio di Stato n. 2631 del 29 marzo 2021](#)²⁵. *Facebook* era stata sanzionata dall'Autorità per pratiche commerciali scorrette, per aver ingannato gli utenti presentando il servizio di *social network* come gratuito e celando invece il profilo di sfruttamento economico sotteso alla cessione dei dati da parte degli *users*. Nella sua difesa, la *Big Tech* aveva sostenuto che l'Autorità garante della concorrenza e del mercato non avesse competenza per infliggere una sanzione per pratiche commerciali scorrette in quanto non vi erano profili economici nella cessione di dati degli utenti a *Facebook*, proprio perché i dati personali non sono per loro natura commerciabili, essendo diritti fondamentali, quindi indisponibili. Questa tesi, contrastata dalla controparte, è stata poi scartata in ultima analisi nella decisione del Consiglio di Stato. Alla luce della disciplina dell'altruismo dei dati, sembrerebbe che la previsione della possibilità di cedere i propri dati personali per fini di interesse generale dia una indicazione che muove decisamente nella stessa direzione del Consiglio di Stato, in quanto si assume, aprendo a questa possibilità, che vi sia spazio per atti di disposizione del proprio diritto della personalità (digitale).

Ma vi è di più. Il Considerando n. 45 del *Data Governance Act*, come ricordato, elenca una serie di obiettivi di interesse generale per il cui conseguimento gli interessati potrebbero mettere a disposizione i propri dati su base volontaria. Tra di essi, compaiono, ad esempio, l'assistenza sanitaria, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche europee, il miglioramento della fornitura dei servizi pubblici, o delle politiche pubbliche, il sostegno alla ricerca scientifica.

L'elenco delle materie lascia intendere che i dati che potranno essere ceduti per finalità di altruismo apparterranno con buona probabilità alle c.d. categorie particolari, i dati sensibili, quelli che il GDPR

²² Cfr. [Data Governance Act](#), Considerando n. 45. V. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., in particolare, 986 ss.

²³ V., in proposito, EUROPEAN DATA PROTECTION BOARD, EUROPEAN DATA PROTECTION SUPERVISOR, [Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance \(Data Governance Act\)](#), 10 marzo 2021, 38-39.

²⁴ [Data Governance Act](#), artt. 17 ss.

²⁵ [Cons. Stato, sez. VI, 29 marzo 2021, n. 263](#), Facebook Ireland Limited c. Autorità garante della concorrenza e del mercato. Per una sintesi, cfr. v. PAGNANELLI, *Una "valutazione d'impatto" della privacy sulle Big Tech. Riflessioni a margine della sentenza n. 2631/2021 della sesta sezione del Consiglio di Stato*, in E. Cremona, F. Laviola. V. Pagnanelli (a cura di), *Il valore economico dei dati*, cit., 3 ss.

blinda e tutela in modo più deciso nell'articolo 9²⁶. Quindi, a maggior ragione, se l'altruismo dei dati consente di decidere sui propri dati sensibili e di decidere se cederli o meno, resta allora da discutere sull'opportunità o meno di rendere questa cessione anche in parte remunerativa.

Ocorre, peraltro, sottolineare che, anche in presenza di diritti fondamentali inviolabili, indisponibili e irrinunciabili, sembrerebbe potervi essere spazio per una differenza tra l'estremo della disponibilità giuridica *tout court* di un diritto e possibilità di disporre di alcune facoltà in essa ricomprese. Autorevole dottrina si è già interrogata sulla configurabilità di una distinzione tra la rinuncia alla titolarità e quella all'esercizio di un diritto. La richiama Giorgio Resta, sottolineando che, seppure a seguito di una attenta valutazione in concreto della tipologia di beni coinvolti, delle finalità e degli effetti, resta configurabile un atto giuridico che disciplini le modalità di esercizio di un diritto fondamentale²⁷.

La decisione, quindi, appare più etica e politica che giuridica. Vi è da chiedersi se l'ordinamento nazionale ed europeo sia abbastanza saldo da poter garantire una sicura circolazione dei dati personali, tutelando la corporeità digitale e il diritto fondamentale alla protezione dei dati personali, conservando la loro indisponibilità. La cassetta degli attrezzi è abbastanza fornita, in particolare con i diritti elencati nel GDPR (consenso, limitazione, portabilità, opposizione²⁸) ed ora con i nuovi articolati europei più volte citati. Occorrerà intervenire sulla consapevolezza dell'utilizzo di questi strumenti al fine di rendere effettiva la partecipazione dei cittadini rispetto al destino dei propri dati.

4.2 *Uno sguardo al futuro: il Data Act*

In seno alla "Strategia europea per i dati" nasce anche la proposta di *Data Act*, dichiaratamente al fine di garantire, attraverso regole armonizzate, l'equo accesso ai dati e la distribuzione del valore che essi creano tra tutti gli attori della *Digital Society*.

Come sottolineato nella relazione introduttiva, il valore dei dati è, infatti, concentrato nella disponibilità di poche società. Al contempo, la maggior parte dei dati prodotti e trattati nello spazio giuridico europeo non viene utilizzata²⁹. La Legge sui dati tenta di dare un impulso alla *data economy* europea, ottimizzando l'accessibilità e l'utilizzo dei dati e promuovendo una distribuzione più equa del loro valore, impedendo che le piccole e medie imprese, contraenti deboli, sottoscrivano accordi che non garantiscano loro un accesso adeguato ai dati.

V'è da dire che, sino ad oggi, l'attenzione posta sullo sviluppo del Mercato unico, obiettivo centrale della strategia europea, ha portato la Commissione a concentrare gli interventi sulla

²⁶ L'articolo 9 del GDPR pone un divieto di trattamento per le categorie particolari di dati personali, ovverosia quelle idonee a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il secondo paragrafo contiene invece una serie di discriminanti che, ove presenti, rendono legittimo il trattamento di queste tipologie di dati personali. Compiono in questo elenco il consenso esplicito dell'interessato, l'assolvimento di regole in materia di diritto del lavoro, la tutela di un interesse vitale, i trattamenti effettuati all'interno delle attività di una fondazione o associazione, i casi in cui i dati personali siano stati resi pubblici dall'interessato, i trattamenti necessari per tutelare un diritto in sede giudiziaria, i trattamenti effettuati per motivi di interesse pubblico rilevante, o per finalità di medicina preventiva o di medicina del lavoro, o per motivi di interesse pubblico nel settore della sanità pubblica, di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

²⁷ V. G. RESTA, *Il diritto alla protezione dei dati personali*, in F. Cardarelli, S. Sica, V. Zeno-Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004, 52 ss.

²⁸ Si tratta, *in primis*, delle norme contenute agli articoli da 12 a 22 del Regolamento europeo n. 2016/679. Si vedano in proposito i commentari L. Bolognini, E. Pelin, (a cura di), *Codice della disciplina privacy*, cit.; R. Panetta, (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, Giuffrè, Milano, 2019; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, cit.; G.M. Riccio, G. Scorza, E. Belisario, (a cura di), *GDPR e normativa privacy. Commentario*, cit.

²⁹ [Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo \(Legge sui dati\), COM\(2022\) 68 final](#), Relazione, 1.

progressiva espansione della quota di dati pubblici sottoposti alle regole giuridiche del riutilizzo. Non si era, invece, prestata attenzione alla necessità per il settore pubblico di avere a disposizione più informazioni – tra cui certamente quelle estraibili dai dati di operatori privati – per adempiere in modo più efficiente ai compiti assegnati dalla legge a ciascuna autorità od organismo.

La proposta di *Data Act* affronta in modo incisivo anche la questione della disponibilità dei dati in capo ai soggetti pubblici. L'articolato contiene la disciplina di un meccanismo autoritativo di accesso a *dataset* privati³⁰ da parte di organismi pubblici nei casi di “necessità eccezionale”, come emergenze pubbliche che i soggetti pubblici potrebbero prevenire o gestire grazie ai dati di soggetti privati, che potranno essere utilizzati entro limiti di tempo e di volume. Nella proposta di *Data Act* si contempla anche l'ipotesi in cui la mancanza di dati impedisca alla pubblica autorità di svolgere un compito di interesse pubblico stabilito dalla legge, ove il soggetto pubblico non possa reperire tali dati a prezzi di mercato, né attraverso gli strumenti legislativi in vigore o da adottare. Anche la riduzione dell'onere amministrativo che graverebbe sul soggetto pubblico nel caso di reperimento dei dati con modalità alternative viene considerata una condizione sufficiente per procedere all'accesso ai dati “d'imperio”.

A fronte della messa a disposizione dei dati da parte dei soggetti privati, il *Data Act* prevede, che la richiesta dovrà specificare quali siano i dati richiesti, a quale scopo, l'uso che se ne farà, il tempo di utilizzo³¹. L'autorità pubblica richiedente dovrà, inoltre, indicare la base giuridica della richiesta e dimostrarne l'eccezionalità, oltre che il termine entro il quale i dati debbono essere resi disponibili. La messa a disposizione dei dati per rispondere ad una emergenza pubblica non prevede il pagamento di alcun corrispettivo. Il compenso non potrà superare i costi tecnici ed organizzativi sopportati dal titolare per rispondere alla richiesta³².

5. Conclusioni

Le potenzialità di utilizzo di strumenti di premiali per aumentare l'*engagement* dei cittadini nella cura dei beni pubblici e nello sviluppo di servizi migliori sono elevate e stimolano l'interesse degli amministratori pubblici che immaginano utilizzi virtuosi di questi sistemi tecnologici innovativi.

Il Garante per la protezione dei dati personali ha ritenuto di porre peraltro sotto osservazione diverse iniziative di tipo premiale promosse in alcuni enti locali italiani sulla base di meccanismi di *scoring*. La “cittadinanza a punti” nei casi oggetto di analisi da parte del Garante era utilizzata per la migliore gestione della mobilità, per l'assegnazione di alloggi di edilizia residenziale pubblica, per attivare strumenti come lo *smart citizen wallet* del cittadino. A fronte dell'indubbio valore - in termini di efficienza, efficacia ed economicità dell'azione pubblica – delle sperimentazioni richiamate, l'Autorità ha ritenuto di aprire delle istruttorie per verificare le modalità di realizzazione delle stesse. Restano infatti alti e non possono essere messi da parte i rischi connessi a meccanismi di profilazione da cui potrebbero derivare conseguenze giuridiche negative per i diritti e le libertà degli interessati, inclusi i soggetti più vulnerabili³³.

Sul versante della valorizzazione dei dati nella migliore elaborazione delle politiche pubbliche, il *Data Governance Act* (nella parte relativa all'altruismo dei dati) e il *Data Act* (nella parte che prevede la possibilità per le autorità pubbliche di accedere d'imperio a dati dei privati) sembrerebbero riequilibrare scelte strategiche che sono state sin qui volte principalmente a garantire lo sviluppo delle imprese e del mercato e sono state meno preoccupate di assicurare al contempo l'efficienza della infrastruttura pubblica. Questa differenza di approccio tra il settore pubblico e il privato emerge anche dalla lettura del documento *Shaping Europe's Digital Future*, pubblicato il 19 febbraio 2020, in

³⁰ G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., in particolare, 980.

³¹ [Proposta di Data Act](#), art. 17.

³² [Proposta di Data Act](#), art. 20.

³³ V. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, “Cittadinanza a punti”: Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini “virtuosi”, 8 giugno 2022, [docweb n. 9778361](#).

occasione della presentazione della “Strategia europea dei dati”. In esso prevalgono i temi dello sviluppo del *Digital Single Market*, mentre il settore pubblico viene citato solo genericamente rispetto alla difesa della democrazia e della genuina formazione dell’opinione pubblica³⁴.

Insieme all’altruismo dei dati disciplinato nel *Data Governance Act*, l’obbligo di messa a disposizione svolge ora finalmente una funzione di riequilibrio tra il costante aumento del volume – e dunque del valore – dei dati in possesso di pochi, grandi operatori privati, e la scarsità di dati dei privati a disposizione del settore pubblico³⁵, attraverso scelte normative di cui nei prossimi anni dovranno essere verificati legittimità (specie per il *Data Act* non ancora approvato) ed efficacia. Alla luce dello scenario appena tratteggiato, il percorso della valorizzazione dei dati in ambito pubblico è ancora tutto da scrivere.

³⁴ EUROPEAN COMMISSION, *Communication: Shaping Europe’s digital future*, 19 febbraio 2020.

³⁵ Ivi, 3: «[...] la Commissione presenta una proposta di normativa sui dati con l'intento di garantire un'equa ripartizione del valore dei dati tra gli operatori dell'economia dei dati e di promuovere l'accesso ai dati e il relativo utilizzo».