Chiarella ML, Borgese M, 'Regole armonizzate per l'accesso e l'utilizzo dei dati: le novità del recente Data Act' (2024) Special Issue EJPLT.
DOI:

EJPLT
ISSN 2704-8012



Regole armonizzate per l'accesso e l'utilizzo dei dati: le novità del recente Data Act

Harmonized rules for data access and use: the latest news from the recent Data Act

MARIA LUISA CHIARELLA
Professore associato
Università Magna Græcia di Catanzaro

MANUELA BORGESE
Dottorando di ricerca
Università Magna Græcia di Catanzaro

Abstract
Il ruolo delle tecnologie e delle strategie data driven è ogni giorno più influente e decisivo, in maniera trasversale e multidisciplinare, per imprese, pubbliche amministrazioni e cittadini. Il costante aumento dei prodotti connessi a Internet e del volume di dati generati costituisce una risorsa fondamentale nell'era del capitalismo digitale. La consapevolezza di ciò è elemento chiave del recente "Data Act", che dà vita ad un quadro normativo europeo basato su regole chiare al fine di disciplinare la condivisione dei dati in tutti i settori economici, sia pubblici che privati, incentivandone il potenziale e, al contempo, improntando maggiori profili di tutela rispetto alle parti coinvolte.

The role of data-driven technologies and strategies is increasingly influential and decisive, in a transversal and multidisciplinary way, for companies, public administrations and citizens. The constant increase in products connected to the Internet and the volume of data generated constitutes a fundamental resource in the era of digital capitalism. Awareness of this is a key element of the recent "Data Act", which gives life to a European regulatory framework based on clear rules in order to regulate data sharing in all economic sectors, both public and private, encouraging its potential and, at the same time, establishing greater protection profiles for the involved parties.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at:
https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Economia dei dati; Governance europea; Circolazione; Condivisione; Interoperabilità

Summary: 1. Introduzione. – 2. Ricostruzione del quadro normativo. – 3. Premesse introduttive sul Data Act. – 4. Il Data Act: luci ed ombre nella rivoluzione dei dati europee. – 4.1. Integrazione del Data Act nel quadro normativo europeo e con la normativa privacy. – 5. *Focus* sulle clausole abusive. – 6. Conclusioni.

1. Introduzione.*

A quasi tre decenni dall'emanazione della prima direttiva[1], la fisionomia del quadro regolatorio in materia di privacy è molto cambiata di riflesso al processo di datificazione della realtà e alle svolte epocali che questo ha comportato[2].

Il legislatore comunitario, in risposta alla frammentazione normativa nazionale, si è mosso nel senso di una marcata armonizzazione della materia, mediando tra una tutela stringente dei diritti e delle libertà fondamentali e le esigenze di implementazione del mercato interno, nella ferma consapevolezza dell'importanza della libera circolazione e valorizzazione dei dati per il sistema nel suo complesso[3].

Nella realtà contemporanea, in particolare, elemento fondamentale per l'economia digitale è rappresentato proprio dai dati personali e non personali. Le evidenze, peraltro, dimostrano che la maggior parte di questi rimane inutilizzata o accessibile solo ad un ristretto numero di grandi aziende.

Si tratta di uno strumento ormai indispensabile nel mondo del *business* per migliorare la performance aziendale, orientare i processi decisionali, sviluppare analisi e strategie e raggiungere sempre nuove frange di mercato. In ragione di ciò, le politiche dell'UE, in particolar modo negli ultimi dieci anni, hanno posto l'accento sulla creazione di un quadro normativo specifico per regolare la gestione dei dati, favorendone la libera circolazione[4].

Se l'obiettivo è ottenerne il pieno sfruttamento, si mira al contempo ad agevolare l'equilibrio e la trasparenza del mercato, soprattutto a vantaggio delle piccole e medie imprese che si trovano in condizioni di dipendenza rispetto alle grandi piattaforme digitali. Ciò presuppone, nello specifico, la

* Il paper è frutto di riflessioni comuni delle autrici; nello specifico, sono di M.L. Chiarella i par. 1, 2 e 5, di M. Borgese i par. 3, 4, 4.1 e 6.

[1] Direttiva n. 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[2] Si v., *ex plurimis*, I.A. Caggiano, *Il consenso al trattamento dei dati nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Politica del diritto*, 2018, 1, 67 ss.; L. Gatt, R. Montinari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, *ivi*, 2017, 2, 363 ss.; S. Torregiani, *Il* Data Act*: una versione europea del* Data Nationalism*?*, in *Riv. it. inf. e dir.*, 2023, 2, 132 ss.

[3] In argomento, v. G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, 971 ss.

[4] Si v. in tal senso la Comunicazione della Commissione europea "*Costruire un'economia dei dati europea*", COM (2017/09 final), preceduta dalla Comunicazione "*Verso una florida economia basata sui dati*", COM (2014/442 final).

creazione di un sistema di governance nei settori strategici e di interesse pubblico e privato che rafforzi la fiducia degli utenti nelle dinamiche di mercato.

Come attesta la comunicazione della Commissione europea "Una strategia europea per i dati" [5], si vuole rendere l'UE leader, a livello economico e tecnologico, nella società contemporanea, tenendo conto che "i dati sono la linfa vitale dello sviluppo economico". Il programma di lavoro della Commissione stabilisce diversi obiettivi strategici, tra cui si pone *in primis* una libera circolazione dei dati a livello settoriale e intersettoriale. Si mira a costruire un governo dei dati, basato sui valori europei, che promuova l'equità, la trasparenza, la sicurezza, la non discriminazione, la responsabilità, l'interoperabilità, la condivisione, l'accesso e la portabilità[6].

Da menzionare, in tale ambito, è anche la risoluzione del 31 marzo 2021[7], ove si esorta la Commissione "a presentare una legge sui dati per incoraggiare e consentire in tutti i settori un flusso di dati più ampio ed equo da impresa a impresa (B2B), dall'impresa alla pubblica amministrazione (B2G), dalla pubblica amministrazione all'impresa (G2B) e da pubblica amministrazione a pubblica amministrazione (G2G)". Nella risoluzione si evidenzia che la strategia costituirà un prerequisito per la sostenibilità delle imprese europee e la loro competitività globale, definendo le condizioni e stabilendo il ruolo guida dell'Unione nell'economia dei dati.

Il risultato atteso è un contesto rinnovato, contraddistinto da servizi migliori, crescita sostenibile e consumo energetico più consapevole. Il quadro regolatorio emergente mira a disegnare una società digitale in cui si possano perseguire plurimi obiettivi: potenziare il mercato unico digitale, contribuendo alla sovranità economica e digitale europea[8], mantenendo ferma la tutela dei diritti fondamentali nella persona[9].

Come rilevato nella risoluzione del 2021, centrale, nella riuscita di tali obiettivi, è la fiducia nei servizi digitali e nella sicurezza dei prodotti intelligenti, affinché il mercato unico digitale possa crescere e prosperare; ciò è fattore prioritario sia nelle politiche pubbliche che nei modelli imprenditoriali. La risoluzione fa leva inoltre sull'importanza di interoperabilità, portabilità e di

---

[5] 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 (Bruxelles, 19.2.2020): "L'obiettivo è creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale. Dovrebbe trattarsi di uno spazio nel quale il diritto dell'UE possa essere applicato con efficacia e nel quale tutti i prodotti e i servizi basati sui dati siano conformi alle pertinenti normative del mercato unico dell'UE. Quest'ultima dovrebbe a tal fine combinare una legislazione e una governance idonee allo scopo per garantire la disponibilità dei dati, investendo in norme, strumenti e infrastrutture, come pure in competenze per la gestione dei dati. Un simile contesto favorevole, che offre incentivi e maggiori possibilità di scelta, comporterà un aumento dei dati conservati ed elaborati nell'UE".

[6] Cfr. G. CERRINA FERRONI, *Luci e ombre della Data Strategy europea*, in *Agendadigitale.eu*, 12 maggio 2022. Sul diritto alla portabilità, v. la riflessione di C. COLAPIETRO, *Il diritto alla portabilità dei dati e l'evoluzione del quadro normativo,* in *dirittifondamentali.it,* 2023, 2, 1 ss.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0098&from=EN.

[8] Sui problemi connessi alla perimetrazione del concetto di sovranità secondo il nuovo significato assunto nell'epoca della datificazione, v. S. TORREGIANI, *Il* Data Act*: una versione europea del* Data Nationalism*?,* cit., 131 ss.

[9] F. PIZZETTI, *Introduzione alla regolazione europea della società digitale*, in ID. (a cura di), *La regolazione europea della società digitale*, Torino, 2024, 1 ss.

infrastrutture aperte, per contrastare abusi del potere di mercato da parte di attori dominanti. I mercati digitali sono, infatti, caratterizzati da elevate barriere all'ingresso relative all'accesso e alla proprietà dei dati. Regolamentarne la condivisione e sbloccare i relativi mercati può rappresentare un possibile modo per correggere queste carenze[10].

Tutto questo è costantemente preso in considerazione negli interventi dell'UE. In questo contesto, il Data Act[11], oggetto della presente riflessione, rappresenta un pilastro fondamentale e la seconda grande iniziativa di regia comunitaria (dopo il Data Governance Act). Il fine perseguito è la creazione di un quadro di normazione intersettoriale, intervenendo su questioni che influenzano le relazioni tra gli attori dell'economia dei dati.

Sullo sfondo, vi sono i princìpi per la transizione digitale, secondo i valori costituzionali europei, messi a fuoco nella recente *Dichiarazione sui diritti e principi digitali europei* approvata nel mese di gennaio 2023. La Dichiarazione illustra l'impegno dell'UE a favore di una trasformazione digitale sicura, protetta e sostenibile che ponga al vertice la dignità umana e i diritti fondamentali, in conformità a quanto già solennemente proclamato nel Preambolo della Carta dei diritti fondamentali dell'Unione europea. Si certifica, in tal modo, l'impegno politico dell'UE e dei suoi Stati membri di promuovere e attuare questi princìpi in tutti gli ambiti coinvolti dal processo di digitalizzazione, quale bussola per l'Agenda Digitale Europea del decennio 2030. In questo programma politico, si stabilisce un modello di cooperazione tra gli Stati membri e le istituzioni europee per conseguire le finalità stabilite per il decennio digitale alla luce dei princìpi e dei diritti sanciti nella Dichiarazione.

2. Ricostruzione del quadro normativo.

Pare qui opportuno, a livello introduttivo, tracciare le coordinate del contesto normativo generale volto a valorizzare l'implementazione del sistema europeo di governo dei dati, di cui il recente Data Act è parte integrante[12].

A tal fine, è utile risalire nel tempo e ricostruire l'architettura normativa europea in materia, dai primi provvedimenti ad oggi[13]. Giova, al riguardo, tener conto del fatto che se la Carta dei diritti fondamentali dell'UE ha sancito il diritto di ogni individuo alla protezione dei propri dati personali (art. 8), distinguendolo dal diritto alla riservatezza (art. 7), la protezione delle persone fisiche rispetto al trattamento dei dati personali che le riguardano si ha anche

[10] M. SZCZEPAŃSKI, *Is data the new oil? Competition issues in the digital economy*, European Parliament Research Service, January 2020.
[11] Si v. il recente commento di A. RICCI, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *Nuove Leggi Civ. Comm.*, 2024, 4, 799 ss.
[12] Si v. il recente commento a cura di M. HENNEMANN, G.K. EBNER, B. KARSTEN, G. LIENEMANN, M. WIENROEDER, *Data Act. An introduction*, Nomos, 2024.
[13] Sono ancora attuali le riflessioni di C.M. BIANCA, *Note introduttive*, in C.M. BIANCA, F.D. BUSNELLI, *La protezione dei dati personali, Commentario al D. Lgs. 30 giugno 2003, n. 196*, Padova, 2007, XIX ss.; F.D. BUSNELLI, *Note introduttive II. Dalla legge al "codice": un dilemma, una sfida, un consolidamento normativo, una (imperfetta) razionalizzazione delle tutele, ivi*, XIX ss. e di F. BASILICA, *Note introduttive III. Il difficile percorso della formalizzazione giuridica dei diritti della personalità c.d. atipici*, *ivi,* IXI ss.

nel Trattato sul funzionamento dell'Unione europea (art. 16), che costituisce una base giuridica specifica per l'adozione di atti legislativi in materia.

Storicamente, la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali[14] è stata il primo documento internazionale vincolante a tutela dell'individuo contro possibili abusi nella raccolta e nel trattamento dei dati personali e dei dati "sensibili" in assenza di adeguate tutele legali. Il preambolo di tale Convenzione richiama "il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica".

Alla Convenzione sono, inoltre, riconducibili alcuni capisaldi dell'attuale normativa privacy, come la stessa definizione di dato personale e di trattamento automatizzato, la individuazione di categorie speciali di dati meritevoli di specifiche garanzie, la sicurezza quale principio base del trattamento, il diritto di accesso e di rettifica. La Convenzione ha inoltre ammesso restrizioni ai diritti in presenza di interessi prevalenti (quali, ad esempio, sicurezza dello Stato, repressione dei reati, etc.) e ha imposto alcune restrizioni ai flussi transfrontalieri in mancanza di protezione equivalente.

Spostando l'attenzione sul diritto europeo derivato, durante l'ultimo decennio del XX secolo, nel contesto di una tutela armonizzata dei diritti fondamentali, la già ricordata Direttiva n. 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[15]) ha avuto il merito di abbattere le frontiere per garantire un libero flusso di dati, prestando tutela alle persone fisiche nell'equilibrio tra protezione personale e libera circolazione dei dati all'interno dell'UE, in un'ottica di tutela dell'innovazione e del diritto fondamentale dell'individuo al controllo delle informazioni che lo riguardano[16].

Nel 2002, si è avuta l'emanazione della Direttiva E-privacy che introduceva strumenti di regolazione più specifici nel campo delle comunicazioni elettroniche[17], comprese le norme relative alla memorizzazione e all'accesso di dati personali e non personali dalle apparecchiature terminali. Nel 2006, invece, vengono introdotte regole per la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[18].

A seguito dello sviluppo tecnologico e della diffusione delle attività *online*, nel 2009 si avvia un processo di consultazione, ad opera della Commissione europea, al fine di adottare un regolamento e consentire una piena armonizzazione in materia di protezione dei dati personali, al tempo

[14] Strasburgo, 28 gennaio 1981.
[15] Recepita nel nostro ordinamento con la legge 31 dicembre 1996, n. 675, poi abrogata dal D. Lgs. 30 giugno 2003, n. 196 (Codice privacy). V. sul punto F. BASILICA, *Note introduttive III. Il difficile percorso della formalizzazione giuridica dei diritti della personalità c.d. atipici*, cit., LXXX; F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, in V. CUFFARO e V. RICCIUTO (a cura di), *La disciplina del trattamento di dati personali*, Torino, 1997, 48 ss.
[16] S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, 19 ss.
[17] Direttiva 2002/58/CE del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, recepita con D. Lgs. 30 giugno 2003, n. 196 (Codice privacy) e successivamente modificata dalla Direttiva 2009/136/CE.
[18] Direttiva 2006/24/CE del 15 marzo 2006 recepita con il D. Lgs. 30 maggio 2008, n. 109.

caratterizzata dalla frammentazione normativa in ragione del fatto che gli Stati membri dell'UE avevano applicato e attuato la direttiva in modi diversi.

Così, nel 2014, è emanato il Regolamento in materia di identificazione elettronica e servizi fiduciari[19] e, due anni dopo, si ha il GDPR (*General Data Protection Regulation*)[20] che, come è ben noto, rappresenta, da un lato, uno strumento di uniformazione del diritto volto ad eliminare le differenze normative nazionali e, dall'altro, uno strumento strategico fondamentale nel contesto del mercato unico digitale[21]. Nel 2018, poi, si ha il Regolamento sulla protezione dei dati per le istituzioni, gli organi e gli organismi dell'Unione Europea[22], che ha fornito le norme applicabili al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e degli organismi dell'UE in linea con gli elevati standard di protezione dei dati prescritti dal GDPR[23]. Ancora, nel 2018, il Regolamento relativo alla libera circolazione dei dati non personali nell'Unione europea ha messo in luce la questione riguardante la disciplina delle informazioni non connesse ad una persona fisica identificata o identificabile[24], con l'obiettivo di facilitarne lo scambio e la creazione di un nuovo mercato.

Nel 2019, tra i documenti normativi rilevanti in materia, si possono menzionare il Regolamento relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (che ha abrogato il Reg. UE n. 526/2013) («regolamento sulla cibersicurezza»)[25], la direttiva Open Data (relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico)[26], il Regolamento P2B che promuove equità e trasparenza per gli

[19] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[20] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Il regolamento è entrato in vigore il 24 maggio 2016 ed è applicato dal 25 maggio 2018, abrogando la Direttiva 95/46/CE per una piena armonizzazione della disciplina in materia di protezione dei dati personali nell'UE. Per tutti, si v. G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove Leggi Civ. Comm.*, 2017, 1, 1 ss. e, più di recente, R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021 (con specifica attenzione al GDPR, si v. pp. 65 ss.).

[21] Nel nostro ordinamento, l'adeguamento della normativa interna al GDPR si è avuto con il Decreto Legislativo n. 101/2018 che ha modificato il Codice Privacy, uniformandolo ai princìpi del GDPR. In argomento, con specifico riferimento al profilo del consenso, v. L. GATT, I.A. CAGGIANO, R. MONTINARI (eds.), *Privacy and consent. A legal and UX&HMI Approach for data protection*, Univerity Suor Orsola Press, 2021, *passim*.

[22] Reg. (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

[23] Il regolamento, che ha abrogato e sostituito il testo precedente [Reg. (CE) 45/2001], si applica dall'11 dicembre 2018.

[24] Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018 su un quadro per la libera circolazione dei dati non personali nell'Unione Europea. In argomento, si v. S. TORREGIANI, *Il dato non personale alla luce del Reg. (UE) 2018/1807*, in *Federalismi*, n. 18, 10/06/2020.

[25] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019.

[26] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 recepita con D. Lgs. 15 dicembre 2021, n. 200.

utenti commerciali dei servizi di intermediazione online[27], nonché la Direttiva Omnibus (la nuova direttiva europea sui diritti dei consumatori)[28].

I recenti interventi normativi, tasselli fondamentali della strategia europea[29] compongono un quadro specifico per l'economia dei dati e mirano ad aumentare la fiducia degli utenti, ad accrescere la disponibilità dei dati e a superare gli ostacoli tecnici al loro riutilizzo neutralizzando il rischio di *lock-in* per consumatori e imprese[30].

A completamento di ciò, si è avuto più di un intervento rilevante in materia: il Regolamento sui dati, oggetto della presente indagine (*Data Act* - in vigore dall'11 gennaio di quest'anno) [31] ; quello sulla Governance dei dati (*Data Governance Act*)[32]; sui servizi digitali (*Digital Service Act*)[33]; sui mercati digitali (*Digital Market Act*)[34], per arrivare al regolamento sull'intelligenza artificiale (*Artificial Intelligence Act*)[35] e al recente regolamento sulla interoperabilità dei sistemi informativi e di rete per favorire l'interoperabilità transfrontaliera dei servizi pubblici digitali transeuropei (*Interoperable Europe Act* [36]). I provvedimenti menzionati delineano uno scenario normativo in cui è presente un bilanciamento tra il crescente *favor* verso la circolazione dati (personali e non) e la protezione del diritto fondamentale della persona ad avere il controllo sugli stessi.

Dall'evoluzione normativa, sinteticamente tratteggiata, emerge il passaggio da un modello "unipolare" (di tutela costituzionale dell'autodeterminazione informativa) alla introduzione di un vero e proprio sistema "multipolare" di *governance* dei dati (personali, non personali e di natura mista) [37] volto a

---

[27] Regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio del 20 giugno 2019.

[28] Direttiva (UE) 2019/2161 del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, recepita con D. Lgs. 18 marzo 2023, n. 26.

[29] In argomento si veda G. CERRINA FERONI, *Luci e ombre della Data Strategy europea*, cit.

[30] V., per tutti, P. STANZIONE, *I poteri privati delle piattaforme e le nuove frontiere della privacy*, Torino, 2022; V. ZENO ZENCOVICH, *Do "data markets" exist?*, in G. RESTA - V. ZENO ZENCOVICH (a cura di), *Governance of /trough Big Data*, I, Roma, 2023, 415 ss.; A. QUARTA - G. SMORTO, *Diritto privato dei mercati digitali*, Firenze, 2024, XI ss..; Ł.D. DĄBROWSKI - M. SUSKA (eds.), *The European Union Digital Single Market. Europe's digital Transformation*, London and New York, 2022, 1 ss.

[31] Regolamento (UE) 2854/2023 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828.

[32] 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.

[33] 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.

[34] 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.

[35] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

[36] Regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio del 13 marzo 2024 che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile) che stabilisce misure che promuovono l'interoperabilità transfrontaliera dei servizi pubblici digitali transeuropei, contribuendo in tal modo all'interoperabilità dei sottostanti sistemi informativi e di rete, definendo norme comuni e un quadro di governance.

[37] Si tratta di un modello "nel quale le istanze di protezione dei dati coesisteranno con parti dignità con quelle di libero accesso e riuso dei dati medesimi" (cfr. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 975). Per l'esame delle problematiche connesse a questa metamorfosi,

consentirne il migliore sfruttamento, potenziando così la competitività del sistema europeo nei mercati internazionali [38]. Emerge, altresì, un quadro normativo fortemente mirato verso la valorizzazione del valore economico del dato, quale "nuovo petrolio"[39].

Conferma di quest'ultimo assunto, sul piano normativo, si rinviene nel fatto che i dati personali possono costituire il corrispettivo della fornitura di contenuti o servizi digitali e che a tali contratti si applicano tutte le tutele accordate ai consumatori[40].

3. Premesse introduttive sul Data Act.

Negli ultimi anni si è assistito ad un notevole aumento dei dispositivi connessi e ad una maggiore interazione con questi, a cui è corrisposto un proporzionale aumento dei dati generati. Si tratta di una tendenza destinata a crescere: secondo le stime previsionali della Commissione Europea, entro il 2025 il volume globale di dati aumenterà del 530%, per un valore economico di 829 milioni di euro[41].

Al di là degli indici strettamente numerici, non vi è dubbio che i dati rappresentino un elemento di imprescindibile valore strategico, in virtù del loro elevato potenziale nel contesto della transizione digitale ed ecologica.

---

ancora *in progress*, dell'impianto normativo: v., *ex plurimis*, G. FINOCCHIARO, *Commento all'art. 1 GDPR,* in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, cit., 113 ss.; V. RICCIUTO, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, 105 ss.; ID., *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 2, 643 ss.; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dr. inf.*, 2018, 689 ss.; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, *passim*; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, 27 ss.; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 9 ss.; C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, 2021, 39. Una (seppur diversa) "tensione" tra "due anime confligenti, portatrici delle opposte esigenze di tutela della riservatezza e di tutela dell'informazione" era stata percepita già nel Codice privacy da C.M. BIANCA, *Note introduttive*, cit., XXXI.

[38] Di *cambio di paradigma valoriale: dalla protezione alla valorizzazione dei dati* discorre A. RICCI, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, cit., 799. In argomento, si v. le riflessioni di I.A. CAGGIANO, *Il consenso al trattamento dei dati personali tra nuovo Regolamento e analisi comportamentale*, in *Annali. Rivista di Ateneo*, 2016-2018, 7 ss.: F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e Impresa Europa*, 2021, 1, 199 ss.; T.M. UBERTAZZI, *European strategy for data and Artificial Intelligence Act. A functional perspective*, in *Contratto e impresa Europa*, 2023, 3, 429 ss.

[39] C. HUMBY, *The world's most valuable resource is no longer oil, but data*, in *The Economist*, 6 maggio 2017. In prospettiva opposta, si veda A.G. MARTINEZ, *No, Data Is Not the New Oil*, in Wired, February 2019.

[40] Si vedano, in tal senso, gli artt. 135-*octies* e 46, comma 1-*bis,* del Codice del Consumo, introdotti dal decreto legislativo 4 novembre 2021, n. 173 di attuazione della Direttiva UE 2019/770 e dal decreto legislativo 7 marzo 2023, n. 26 di attuazione della Direttiva UE 2019/2161. In giurisprudenza, si v. Cons. Stato 29 marzo 2021, n. 2631 (in *Resp. civ. prev.,* 2021, 5, 1604) di conferma della pronuncia del T.A.R. Lazio 10 gennaio 2020, n. 260 (pubblicata in *Giur. it.*, 2021, 320 ss., con nota di C. SOLINAS, *Circolazione dei dati personali, onerosità e pratiche commerciali scorrette*).

[41] Analisi contenuta nella sezione istituzionale del sito della Commissione Europea, (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en) dedicato alla strategia europea sui dati.

Al riguardo, si è rilevato che le aziende che basano i propri piani di innovazione sui dati registrano una crescita della produttività del 5% - 10% più rapida rispetto ad altre[42].

In un contesto di indubbie opportunità, però, osserviamo che tale potenziale non viene pienamente sfruttato, per diverse ragioni.

Innanzitutto, la gestione di grandi fonti di dati richiede ingenti investimenti per la creazione ed il mantenimento di adeguate infrastrutture tecnologiche.

In secondo luogo, per sfruttare appieno il volume dei dati, è fondamentale possedere specifiche competenze digitali. Purtroppo, le statistiche europee, fra queste l'indice DESI[43], registrano ancora una situazione carente e su cui sono necessari interventi mirati.

Altri ostacoli sono di tipo normativo, considerata la mole di adempimenti richiesti per la *compliance*, spesso al di fuori della portata delle aziende soprattutto quelle di fascia medio-piccola.

La situazione attuale, quindi, vede il potere di sfruttamento dei dati concentrato nelle mani di poche realtà imprenditoriali, che per dimensioni e capacità economica, sono riuscite ad oltrepassare gli ostacoli sopra evidenziati.

Questa circostanza introduce un ulteriore limite per le piccole e medie imprese, rappresentato dalla presenza di posizioni dominanti che si traducono, molto spesso, in rapporti contrattuali sbilanciati o in mercati inaccessibili a causa delle concentrazioni dei dati nelle mani dei *big player.*

Il quadro esaminato evidenzia la persistenza di forti esigenze di intervento, alla base delle quali si trova il Data Act, parte integrante della già descritta strategia europea sui dati[44].

A seguito di un complesso iter legislativo, il Data Act ("DA"), Regolamento 2023/2854/UE, è stato pubblicato in Gazzetta Ufficiale il 23 dicembre 2023[45], divenendo applicabile quasi integralmente a partire dal 12 settembre 2025, salvo le deroghe specificamente indicate[46].

L'articolato normativo mira a perseguire una serie di obiettivi, evidenziati in 119 considerando, al fine di dare impulso ad un sistema di governance dei dati anche nei settori più critici[47].

---

[42] E. BRYNJOLFSSON, L.M. HITT, H. HELLEN KIM, *Strength in Numbers: How Does Data-Driven Decision making Affect Firm Performance?* (April 22, 2011). Consultato sulla piattaforma SSRN: https://ssrn.com/abstract=1819486 or http://dx.doi.org/10.2139/ssrn.1819486.

[43] Indice dell'economia e della società digitali (DESI): https://digital-strategy.ec.europa.eu/it/policies/desi.

[44] V. in argomento, S. TORREGIANI, *Il* Data Act*: una versione europea del* Data Nationalism*?,* cit., 138 ss.

[45] Si v. https://eur-lex.europa.eu/eli/reg/2023/2854/oj, https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts.

[46] Art. 50 Data Act: "Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Esso si applica a decorrere dal 12 settembre 2025. L'obbligo derivante dall'articolo 3, paragrafo 1, si applica ai prodotti connessi e ai servizi correlati immessi sul mercato dopo il 12 settembre 2026. Il capo III si applica solo in relazione agli obblighi di messa a disposizione dei dati a norma del diritto dell'Unione o della legislazione nazionale adottata in conformità del diritto dell'Unione, che entrano in vigore dopo il 12 settembre 2025. Il capo IV si applica ai contratti conclusi dopo il 12 settembre 2025. Il capo IV si applica a decorrere dal 12 settembre 2027 ai contratti conclusi il o anteriormente al 12 settembre 2025, a condizione che: a) siano a tempo indeterminato; o b) scadano almeno 10 anni dopo l'11 gennaio 2024.

[47] Tra tutti, giova, in particolare, menzionare il Considerando 5: "Il presente regolamento garantisce che gli utenti di un prodotto connesso o di un servizio correlato nell'Unione possano accedere tempestivamente ai dati generati dall'uso di tale prodotto connesso o servizio correlato e che tali utenti possano utilizzare i dati, anche condividendoli con terzi di loro scelta. Esso impone ai titolari dei dati l'obbligo di mettere i dati a disposizione degli utenti e dei terzi scelti dagli utenti in determinate circostanze. Garantisce inoltre che i titolari dei dati mettano i dati a disposizione dei destinatari dei dati nell'Unione a condizioni eque,

A livello introduttivo, appare utile inquadrare il contesto della normativa attraverso una sommaria analisi della relativa struttura.

In particolare, i Capi in cui si articola il DA riguardano: le disposizioni generali (I), la condivisione dei dati da impresa a consumatore e da impresa a impresa (II), gli obblighi per i titolari dei dati tenuti a mettere a disposizione i dati a norma del diritto dell'Unione (III), le clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo tra imprese (IV), le disposizioni concernenti la messa a disposizione dei dati sulla base di necessità eccezionali (V), il passaggio fra servizi di trattamento dei dati (VI), l'accesso governativo e il trasferimento internazionale di dati non personali (VII); l'interoperabilità (capo VIII); le norme di attuazione e di esecuzione (IX); il diritto "*sui generis*" a norma della direttiva 96/9/CE (X) e, da ultimo, le disposizioni finali (XI).

4. Il Data Act: luci ed ombre nella rivoluzione dei dati europea.

Il DA è contraddistinto da una portata rivoluzionaria e rappresenta un vero e proprio perno all'interno della strategia europea sui dati, strumentale ad aumentare il volume dei dati disponibili e a determinare un aumento stimato di 270 miliardi di euro del PIL degli stati UE entro il 2028.

La realizzazione dei princìpi stabiliti dal DA rappresenta[48], nel contesto comunitario, un fattore di sviluppo fondamentale per il mercato digitale interno, a vantaggio della competitività, dell'innovazione e della crescita economica sostenibile. Per favorire questi obiettivi, la politica dell'UE opta per l'armonizzazione giuridica – attraverso l'introduzione di un regolamento UE – bypassando la frammentazione delle legislazioni nazionali ed introducendo regole specifiche in materia di identificazione di chi ha il diritto di utilizzare i dati raccolti, ottenuti o altrimenti generati da prodotti connessi o servizi digitali.

Per inquadrarne concretamente la dimensione, pare opportuno mettere a fuoco i principali obiettivi strategici.

Il primo è certamente quello di facilitare l'accesso e l'utilizzo dei dati, agevolandone la condivisione e, quindi, creando un meccanismo di produzione e di circolarità *by default*, che incentivi sistematicamente i conseguenti benefici, di cui si è già accennato. Centrale è la finalità di equilibrare la posizione contrattuale degli operatori economici, per contribuire alla regolazione di un

---

ragionevoli e non discriminatori e in modo trasparente. Le norme di diritto privato sono fondamentali nel quadro generale della condivisione dei dati. Il presente regolamento adegua pertanto le norme di diritto contrattuale e impedisce lo sfruttamento degli squilibri contrattuali che ostacolano l'accesso equo ai dati e il loro utilizzo. Il presente regolamento garantisce inoltre che i titolari dei dati mettano a disposizione degli enti pubblici, della Commissione, della Banca centrale europea o degli organismi dell'Unione, ove vi sia una necessità eccezionale, i dati necessari per lo svolgimento di un compito specifico nell'interesse pubblico. Il presente regolamento mira altresì ad agevolare il passaggio tra servizi di trattamento dei dati e a migliorare l'interoperabilità dei dati e dei meccanismi e servizi di condivisione dei dati nell'Unione. È opportuno non interpretare il presente regolamento come un atto che riconosce o che conferisce ai titolari dei dati un nuovo diritto di utilizzare i dati generati dall'uso di un prodotto connesso o di un servizio correlato".

[48] Study on the Open Data Directive, Data Governance and Data Act and their possible impact on research, 2022,https://op.europa.eu/en/publication-detail/-/publication/a313139b-1147-11ed-8fa0-01aa75ed71a1. V. le riflessioni di G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 989 ss.

mercato in cui prevalgano l'equilibrio, la trasparenza e le regole della concorrenza, contrastando condotte abusive.

Oltre alla tutela delle imprese, nel DA si riafferma il principio di controllo dei *data subjects* riguardo ai propri dati[49] e con ciò si tutela anche il singolo, come fornitore di dati, utente e consumatore, integrando così la tutela di provenienza consumeristica (art. 1, par. 9).

Si dà vita, mediante il DA, ad un contesto circolare, in cui i dati sono più liberi di fluire in ambienti interconnessi e interoperabili, secondo regole certe ed efficaci.

Poiché il presente contributo non si occupa della condivisione dei dati da imprese a PA[50], si andranno ad esaminare specifici profili normativi di maggiore impatto nel sistema economico-produttivo[51], soprattutto rispetto ai dati generati nel contesto di prodotti connessi e servizi correlati, dell'Internet of Things,[52] con riferimento all'attività dei fornitori di servizi di trattamento dei dati in cloud.

In tale ambito, il DA mira ad incentivare la circolazione di una maggiore quantità di dati, personali e non, consentendo ad imprese e consumatori l'accesso ai dati ottenuti o generati dall'utilizzo di un prodotto connesso o di un servizio correlato, con la possibilità di utilizzarli o cederli a soggetti terzi indicati dall'utente.

Il fine principale è quello di sbloccare il valore economico ed informativo contenuto nei dati stessi, stabilendo un chiaro sistema di regole fra i soggetti (coinvolti ed) indicati nelle definizioni di cui all'art. 2 DA[53]: *l'interessato*, *i.e.* il soggetto i cui dati personali sono trattati, nella definizione dell'art. 4.1 GDPR (11); *l'utente*, quale soggetto 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 (12); *il titolare dei dati*, che ha il diritto o l'obbligo 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 (13); *il destinatario dei dati*, quale soggetto a favore del quale i dati sono messi a disposizione (14) e, infine, *il cliente*, cioè il soggetto che ha instaurato un

---

[49] D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, n. 2/2023. Disponibile in: http://www.osservatoriosullefonti.it

[50] Trattasi di argomento denso e affascinante, dalla portata strategica e rivoluzionaria, inquadrato nel Capo V del DA, cui si rinvia.

[51] Cfr. art. 1 DA.

[52] Per una compiuta definizione di *Internet of Things*, appare utile far riferimento a quanto segnalato dal WP29, nell'opinion n. wp223 del 2014: il concetto di Internet degli oggetti (IoT) si riferisce a un'infrastruttura nella quale miliardi di sensori incorporati in dispositivi comuni di uso quotidiano ("oggetti" a sé stanti oppure oggetti connessi ad altri oggetti o persone) sono progettati per registrare, trattare, conservare e trasferire dati e, essendo associati a identificativi univoci, interagiscono con altri dispositivi o sistemi che sfruttano le capacità di collegamento in rete. V. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf.

[53] Art. 2, par. 11) 12) e 13) DA: 11) «interessato»: l'interessato di cui all'articolo 4, punto 1, del regolamento (UE) 2016/679; 12) «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; 13) «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.

rapporto contrattale con un fornitore di servizi di trattamento dei dati con l'obbiettivo di utilizzare uno o più servizi di trattamento dei dati (30).

Per realizzare tale scopo, il DA impone un sistema di regole basato sulla trasparenza e sull'accessibilità alle informazioni, dettando specifici requisiti che devono sussistere fin dalla progettazione dei prodotti o servizi e in tutto il ciclo di vita dei medesimi.

In particolare, è stabilito che, per impostazione predefinita, i prodotti collegati e i servizi correlati siano progettati, fabbricati e forniti in modo tale che i dati del prodotto e i dati dei servizi correlati, compresi i metadati pertinenti necessari per interpretare e utilizzare tali dati, siano facilmente accessibili in modo sicuro e gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e direttamente accessibile agli utenti (art. 3). Si interviene in maniera molto incisiva per quanto attiene agli obblighi informativi, precontrattuali e contrattuali, nei casi di vendita, noleggio o locazione di un prodotto connesso e rispetto alla fornitura di servizi correlati (art. 3, par. 2 e 3).

Il quadro emergente presenta un disegno molto definito dei requisiti di trasparenza, non solo rispetto alla forma, ma anche per quanto riguarda l'elenco di specifici dettagli tecnici e informativi.

In particolare, con riguardo agli obblighi precontrattuali relativi all'acquisto, noleggio o locazione di un prodotto connesso, dovranno essere indicate le informazioni relative alle caratteristiche, al volume e alle modalità di creazione, salvataggio e gestione dei dati prodotti. Si comprende, tra le altre cose, anche la specifica menzione relativa all'accesso, alle condizioni di utilizzo e alla qualità del servizio (art. 3, par. 2).

Analoghe previsioni sono presenti per i servizi correlati, in relazione ai quali vengono considerati tutti i dati prodotti dall'attività dell'utente relativa al prodotto connesso, generati in fase di fornitura dello stesso. Oltre a quanto già esaminato circa la natura e il volume dei dati, vengono imposte specifiche indicazioni circa l'identità del potenziale titolare dei dati e le modalità di comunicazione con le quali è possibile ed agevole contattarlo, le modalità con cui l'utente può richiedere che i dati siano condivisi con terzi e, ove applicabile, terminare la condivisione dei dati (art. 3, par. 3).

Inoltre, a seguito degli accesi dibattiti avvenuti nel corso dell'iter normativo, è stato precisato che deve essere reso noto se il potenziale titolare dei dati è anche titolare del segreto commerciale contenuto nei dati accessibili dal prodotto connesso o generato durante la fornitura di un servizio correlato o, in caso contrario, l'identità dello stesso (art. 3, par. 3, lett. *h*).

La normativa prevede poi un insieme di previsioni per la condivisione dei dati, ottenuti o generati dall'utilizzo di prodotti o servizi correlati, con terzi, con particolare riguardo ai diritti di accesso e utilizzo, prevedendo l'obbligo per il titolare di rendere prontamente disponibili tali dati (art. 5). Tale accesso deve avvenire in maniera semplice, gratuita per l'utente, in formato completo e strutturato, di uso comune e leggibile da dispositivo automatico, nonché in modo continuo e in tempo reale, se applicabile e tecnicamente possibile (par. 1). Eventuali limitazioni dovranno essere previste contrattualmente tra le parti,

salvo casi specificatamente previsti dalla legge tali da compromettere la sicurezza del dispositivo o del servizio stesso[54] .

In ragione della notevole ampiezza del diritto di accesso rispetto al contenuto dei dati, già in sede di negoziato sono emerse notevoli problematiche su possibili prevaricazioni a danno dei segreti commerciali. La perplessità, che di fatto ha costituito una causa di rinvio nell'adozione del testo definitivo, era appunto legata al fatto che limitare il diritto di accesso avrebbe portato a vanificare lo scopo sotteso all'intera normativa. D'altro canto, consentire l'accesso incondizionato avrebbe compromesso la sicurezza dei segreti industriali delle aziende coinvolte. Pertanto, la soluzione adottata si colloca su un livello mediano, prevedendo in generale che i segreti commerciali debbano essere preservati e divulgati solo se i titolari e gli utilizzatori dei dati adottino tutte le misure necessarie per preservarne la riservatezza, soprattutto nel rispetto a terzi (art. 4, par. 6). Pertanto, il detentore del segreto commerciale individua i dati protetti quali segreti commerciali e concorda con l'utente misure proporzionate e necessarie per preservare la riservatezza, quali clausole contrattuali tipo, applicazione di norme tecniche e di codici di condotta o previsioni di rigorosi protocolli di accesso (art. 4, par. 6).

In assenza di tali garanzie o se l'utente non adotta le misure concordate, la richiesta può legittimamente non essere evasa (par. 7). Tuttavia, poiché trattasi di questione estremamente delicata, spetta al titolare dei dati dimostrare che è altamente probabile che dalla divulgazione possa derivare un grave danno economico, nonostante le misure adottate.

Tale disposizione acquista una connotazione ancora più interessante nel contesto di una richiesta da parte dell'utente di condividere dati con soggetti terzi (art. 5).

Il rischio emergente è quello di rivelare segreti commerciali a potenziali *competitor*. Nel bilanciare tale situazione e tutelare i diritti delle parti coinvolte, il DA prevede una clausola di salvaguardia che limita la divulgazione ai soli casi in cui sia necessaria per adempiere allo scopo concordato tra l'utente e il terzo (par. 6). In tal caso, il titolare dei dati (detentore del segreto commerciale) identifica i dati protetti come segreti commerciali e adotta misure adeguate al trasferimento. Anche in questi casi valgono le eccezioni già osservate riguardo all'opposizione, nei casi in cui la divulgazione potrebbe comportare un grave danno economico per l'azienda o la sospensione, se il terzo non dà attuazione alle misure individuate o lede la riservatezza dei segreti commerciali (par. 9).

Trattasi di soluzione inevitabile, in mancanza di previsioni di questo genere l'applicazione del DA potrebbe costituire una fonte di vulnerabilità per l'integrità aziendale. Riguardo agli strumenti giuridici da utilizzare a fronte di una richiesta di accesso o di condivisione, merita una riflessione la circostanza che, probabilmente, ad oggi mancano normative tecniche o codici di condotta cui far riferimento e, pertanto, la soluzione andrà verso la previsione di strumenti contrattuali, che rappresentano un costo e una barriera per le imprese meno strutturate. Tuttavia, posta l'articolata serie di regole ed eccezioni, si dovrà valutare quale sarà l'applicazione pratica da parte dei soggetti coinvolti.

[54] Artt. 4-5 DA.

4.1 Integrazione del Data Act nel quadro normativo europeo e con la normativa privacy.

Il DA si inserisce all'interno della già menzionata "Strategia europea dei dati" contraddistinta dalle innovative normative di cui si è fatta menzione: si tratta di un panorama normativo che si è andato arricchendo di previsioni fondamentali per sostenere il c.d. "Decennio Digitale" di trasformazione europea[55]. Poiché molte di queste normative impattano su diversi livelli di intensità con le disposizioni del DA, pare opportuno riflettere sui rapporti con alcune di esse.

In particolare, il DA si colloca in un comparto normativo in cui troviamo, tra gli altri, anche il *Data Governance Act*[56] ("DGA"), il Regolamento sulla libera circolazione dei dati non personali [57] ed il Regolamento generale sulla protezione dei dati ("GDPR")[58].

Rispetto al DGA, con cui il DA ha la più stretta relazione, si rendono opportune alcune premesse, per meglio chiarire i rapporti fra le due normative, essendo il DA una parte integrante del medesimo[59].

Il DGA arricchisce lo scenario della Direttiva relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico[60], consentendo una maggiore espressività del potenziale informativo detenuto dalla pubblica amministrazione.

Il DGA contiene, infatti, la disciplina dell'accesso ai dati del settore pubblico, degli strumenti tesi a incentivare la condivisione dei dati detenuti da soggetti privati[61] e individua i processi volti a facilitare la condivisione dei dati da parte di imprese, cittadini e imprese pubbliche. Tali disposizioni sono poi state verticalmente integrate nel DA, che ne individua le modalità di una puntuale interazione, per una più armonica applicazione normativa.

Il DGA ha, quindi, creato le basi su cui si fonda il flusso di raccolta previsto dal DA[62], con le sue regole volte a rendere disponibili e fruibili un numero ancora maggiore di dati, in particolare quelli generati dalla fruizione di prodotti

---

[55] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, COM(2021) 118 final.
[56] Regolamento (UE) 2022/868, cit.
[57] Regolamento (UE) 2018/1807, cit.
[58] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
[59] S. TORREGIANI, *Il* Data Act*: una versione europea del* Data Nationalism*?,* cit., 139.
[60] Direttiva (EU) 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.
[61] Si fa riferimento al c.d. "altruismo dei dati", definito dall'art. 2, n. 16, della DGA come «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».
[62] A. DEL NINNO, *Il Regolamento (UE) 2022/868 sulla governance europea dei dati, Commentario pratico al Data Governance Act - DGA*, Key Editore, 2023, 23 e ss.

connessi e servizi correlati, individuando le categorie di soggetti autorizzati ad accedere, utilizzare e disporre di tali informazioni.

Un diverso contesto di interesse, rilevante ai fini della presente analisi, è quello della tutela dei dati contenuti in *database*, per il possibile accesso a fini analitici e statistici disciplinato dalla direttiva 96/9/CE[63]. Tale normativa tutela non solo la struttura della banca dati, ma anche i relativi contenuti, con il c.d. diritto *sui generis*[64].

Benché trattasi di diritto di assoluta rilevanza, bisogna osservare che nel contesto del DA rappresenta un vero e proprio limite, nei termini desumibili dall'ampia descrizione di cui al paragrafo precedente. Come si legge nel Considerando 112 del DA, sussiste il rischio che i titolari di dati contenuti in banche di dati ottenuti o generati mediante componenti fisiche, quali sensori, di un prodotto connesso e di un servizio correlato o di altri dati generati automaticamente rivendichino il diritto «sui generis», ostacolando in tal modo l'effettivo esercizio del diritto degli utenti di accedere ai dati e di utilizzarli e del diritto di condividere i dati con terzi a norma del DA.

Per tale ragione, al fine di prevenire non solo possibili controversie ma anche per non vanificare uno degli obiettivi portanti del Regolamento, il DA introduce un'importante deroga, limitatamente alle sole ipotesi previste dall'art. 43. Tale disposizione esclude l'applicabilità del diritto *sui generis* quando i dati sono ottenuti o generati da un prodotto connesso o un servizio correlato che rientra nell'ambito di applicazione del DA, in particolare in relazione agli articoli 4 e 5. Ciò non pregiudica l'eventuale applicazione del diritto «sui generis» alle banche di dati contenenti dati che non rientrano nell'ambito di applicazione del regolamento, purché siano soddisfatti i requisiti di tutela previsti dalla medesima norma. Infine, è bene evidenziare che in forza del considerando 112, il diritto *sui generis* continua ad applicarsi al di fuori dell'ambito di applicazione del DA, a condizione tuttavia che ciò non comporti una violazione della tutela prevista dalla legge[65].

Ulteriore riflessione non può che essere rivolta al recentissimo AI ACT, che mira a promuovere lo sviluppo e l'impiego dell'IA nell'UE. Nel perseguire il primato europeo nella disciplina di tale settore, l'AI ACT orienta il potenziale di questa tecnologia attraverso una specifica serie di regole a presidio della sicurezza e dei diritti fondamentali alla base dell'ordinamento europeo. L'enorme complesso di vantaggi derivanti dal ricorso a tali tecnologie è difficilmente sintetizzabile [66] , viste le trasversali applicazioni nei diversi contesti economico sociali, industriali e tecnologici.

Si tratta di sistemi di grande versatilità, con impatti di assoluto interesse che consentono alle organizzazioni di automatizzare i propri processi interni con

---

[63] Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati. In argomento, si v. C. SGANGA, *Ventisei anni di direttiva database alla prova della nuova strategia europea per i dati: evoluzioni giurisprudenziali e percorsi di riforma*, in *Il diritto dell'informazione e dell'informatica*, 2022, 3, p. 651 ss.

[64] Cfr. art. 7 della direttiva 96/9/CE. In argomento, si v. la riflessione di L. ZOBOLI, *Il diritto* sui generis *sulle banche dati e l'economia digitale: perché il* Data Act *non basta*, in *Diritto industriale*, 2021, 320 ss.

[65] Sul punto, v. i rilievi di A. RICCI, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, cit., 811.

[66] European Commission: Directorate-General for Economic and Financial Affairs, Simons, W., Turrini, A. and Vivian, L., *Artificial intelligence – Economic impact, opportunities, challenges, implications for policy*, Publications Office of the European Union, 2024.

vantaggi di costo e di risultato, erogare servizi qualitativamente migliori e di automatizzare processi, ripetitivi e costosi, a beneficio di tutti gli interessati[67].

Fra queste due normative esistono diversi punti di contatto, che evidenziano il ruolo cruciale della loro interconnessione. In primo luogo, il corretto funzionamento dei modelli di IA implica il ricorso a grandi quantità di dati[68], raccolti in maniera corretta e intellegibile, necessari per addestrare i propri algoritmi, ampliare i propri set decisionali e poter restituire degli output validi ed attendibili. Inoltre, queste tecnologie sono sempre più spesso presenti in prodotti connessi o servizi correlati (es.: assistenti virtuali, elettrodomestici intelligenti, etc.), potenziandone le performance e le funzionalità.

Da tali brevi considerazioni, si comprende come il DA rappresenti un pilastro fondamentale nella strategia dell'IA, per il potenziamento nella creazione di dati e nel loro legittimo utilizzo, nonché nella creazione di processi, come nel caso dell'interoperabilità, che ne rafforzino la circolazione.

L'aumento di questo potenziale comporta, però, delle importanti conseguenze e dei notevoli sforzi, soprattutto in termini di *compliance* normativa e tecnologica da parte dei soggetti coinvolti, al fine di rispettare le prescrizioni in materia di *risk assessment* di cui all'AI ACT[69].

Altre normative fortemente connesse ai temi trattati dal DA sono quelle in materia di protezione dei dati personali e non, di cui ai regolamenti (UE) 2016/679, 2018/1725, 2018/1807, nonché quella relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, di cui alla direttiva 2002/58/CE (ePrivacy).

Si tratta principalmente di un "effetto" diretto, derivante dalla circostanza che i profili rientranti nell'ambito oggettivo del DA, come l'utilizzo di un prodotto connesso o di un servizio correlato, comportano la generazione e il trattamento di dati personali e non personali, rendendo così applicabili le relative normative.

Il rapporto fra le diverse discipline segue il costante orientamento del legislatore comunitario, relativo all'autonomia della normativa privacy comunitaria ed alla supremazia delle relative previsioni nel contesto del trattamento dei dati personali[70].

Le disposizioni del DA evidenziano chiaramente il ruolo autonomo e predominante di tali normative precisando, al considerando 7 e all'art. 1 par. 5, che viene lasciato impregiudicato il diritto dell'Unione in materia di protezione dei dati personali e della vita privata, in particolare i regolamenti (UE) 2016/679 e (UE) 2018/1725 e la Direttiva 2002/58/CE [71].

---

[67] Parlamento Europeo, *Artificial intelligence: How does it work, why does it matter, and what can we do about it*? e *Opportunities of Artificial Intelligence,*
M.G. PELUSO, *Intelligenza Artificiale e dati di qualità: la tecnologia come valido alleato*, in *Medialaws* v.2/2022, 322 e ss.

[69] M. EBERS, *Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act* (June 19, 2024). Consultato sulla piattaforma SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387.

[70] Si consideri, in tal senso, che il DA ribadisce in più punti i richiami alle disposizioni privacy applicabili e all'esplicita competenza delle Autorità di Controllo privacy, precisando anche, all'art. 37, che le autorità di controllo incaricate di sorvegliare l'applicazione del regolamento (UE) 2016/679 sono competenti per l'applicazione del DA per quanto riguarda la protezione dei dati personali.

[71] Con riguardo, invece, ai rapporti fra normativa GDPR e Direttiva ePrivacy, soprattutto in merito agli specifici ambiti di interazione, si veda il Parere European Data Protection Board n. 5/2019 del 12 marzo 2019, in particolare per quanto concerne competenze, compiti e poteri delle autorità per la protezione dei dati

La diretta conseguenza è che nessuna disposizione del DA può essere applicata o interpretata in modo da ridurre o limitare i diritti protetti da tali normative.

Si tratta di profili fondamentali che tendono a contemperare l'obiettivo del DA, di incrementare il volume di dati prodotto e beneficiare dei relativi contenuti, con i diritti protetti dal GDPR, dalla Direttiva ePrivacy e inevitabilmente coinvolti.

Si discute di questioni complesse che richiedono ulteriori riflessioni su specifici aspetti inerenti agli obblighi imposti dalle rispettive normative[72].

Il primo riguarda il profilo della liceità, principio cruciale e strutturale del Regolamento Generale sulla Protezione dei dati personali, previsto e disciplinato dall'art. 5[73], che fra l'altro impone il rispetto di una valida base giuridica a norma dell'art. 6 GDPR, delle eventuali condizioni di cui all'art. 9 del GDPR, nonché dall'art. 5, par. 3, della Direttiva 2002/58/CE.

Il citato Considerando 7 offre una chiara prescrizione interpretativa laddove evidenzia la piena vigenza delle disposizioni privacy, chiarendo che il DA non costituisce una base giuridica per la raccolta o la generazione di dati personali da parte del titolare dei dati. Pertanto, il trattamento degli eventuali dati personali derivanti dall'uso del prodotto connesso o del servizio correlato continua ad essere condizionato alla previa ed imprescindibile individuazione della corretta base giuridica[74].

Nella rassegna delle ulteriori norme che affrontano l'interessante correlazione fra DA e normativa privacy, emerge il chiaro intento di prevedere specifici criteri di regolamentazione nei possibili ambiti d'impatto per i diritti e le libertà delle persone fisiche tutelati dalla normativa. Si pensi, ad esempio, all'esercizio dei diritti degli interessati, quali l'accesso e la portabilità, consacrati agli artt. 15 e ss., nonché pilastro strutturale del GDPR, nel caso in cui l'utilizzo di un prodotto o di un servizio correlato generi dati personali che si riferiscono all'interessato. Rispetto a tali ipotesi, come anticipato, il DA non pone alcuna deroga, anzi specifica che il trattamento di tali dati è soggetto alle norme stabilite dal GDPR, anche qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati[75]. Tuttavia, con riguardo a tale contesto, ben potrebbe verificarsi che l'accesso venga richiesto

---

https://www.edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_it.pdf.

[72] In argomento, si v., *amplius*, A. RICCI, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, cit., 816 ss.

[73] Cfr. art. 5 GDPR: I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza"); F. BRAVO (a cura di), *Dati personali, protezione, libera circolazione e governance. 1. Principi*, Pisa, 2024.

[74] In questo senso, si v. anche l'art. 4, par. 12, DA.

[75] In tal senso, si consideri il disposto del Considerando 34: "(...) A norma del regolamento (UE) 2016/679, un utente che è l'interessato ha, in determinate circostanze, il diritto di accedere ai dati personali che lo riguardano e tale diritto non è pregiudicato dal presente regolamento. A norma del presente regolamento l'utente che è una persona fisica ha inoltre il diritto di accedere a tutti i dati generati dall'utilizzo del prodotto connesso, personali e non personali. Se l'utente non è l'interessato ma un'impresa, ivi incluso un imprenditore individuale, ma non nei casi di uso domestico condiviso del prodotto connesso, l'utente è considerato un titolare del trattamento. Di conseguenza tale utente che, in qualità di titolare del trattamento, intenda richiedere dati personali generati dall'uso di un prodotto connesso o di un servizio correlato, deve disporre di una base giuridica per il trattamento dei dati come previsto dall'articolo 6, paragrafo 1, del regolamento (UE) 2016/679, come il consenso dell'interessato o l'esecuzione di un contratto di cui l'interessato è parte".

da un utente che non è l'interessato o il titolare del trattamento, ma ad esempio dal titolare dei dati.

Il problema che si porrebbe in tale caso sarebbe quello di inquadrare la liceità del trattamento al di fuori dell'ordinario schema privacy fra titolare ed interessato[76].

Anche in questo caso è il Considerando 7 ad indicare il percorso da seguire, chiarendo che, poiché il DA non costituisce una base giuridica per consentire l'accesso ai dati personali o per metterli a disposizione di terzi, non dovrebbe essere inteso nel senso che conferisce al titolare dei dati un nuovo diritto di utilizzare i dati personali generati dall'uso di un prodotto connesso o di un servizio correlato. L'evasione di eventuali richieste, prosegue il Considerando 7, dovrebbe prevedere un'attenta analisi in termini di liceità del trattamento e l'adozione di misure quali l'anonimizzazione o la selezione dei soli dati personali relativi all'effettivo richiedente.

Analoghe argomentazioni valgono nell'ipotesi di cui all'art. 5 del DA, che riconosce il diritto dell'utente di condividere i dati con terzi, con riguardo al diritto di portabilità[77] nel caso di dati personali coinvolti in tale richiesta[78].

Nel testo del DA esistono comunque molti altri riferimenti alla normativa privacy, non solo per delimitare eventuali contrasti ma anche in funzione integrativa, rispetto a determinati requisiti. Ad esempio, si pensi al riferimento contenuto nel Considerando 24, che impone al titolare di attuare una ragionevole politica di conservazione dei dati, se del caso, in linea con il principio di limitazione della conservazione di cui all'articolo 5, par.1, lettera e)[79], del GDPR e che consenta l'effettiva applicazione dei diritti di accesso ai dati previsto dal DA.

In base alle precedenti considerazioni, appare ragionevole contestualizzare il DA nel sistema giuridico europeo in funzione di armonica integrazione rispetto al sistema generale di protezione dei dati personali e di tutela della vita privata e delle comunicazioni, equilibrando e contemperando i beni giuridici protetti dalle rispettive normative.

5. *Focus* sulle clausole abusive.

Alla base di un contesto di condivisione reale ed equa, è essenziale che non vi siano squilibri di mercato, in relazione all'accesso ai dati e al loro utilizzo, che mettano a repentaglio la contendibilità dei mercati e le posizioni dei *market*

[76] La definizione di titolare del trattamento è prevista dall'art. 4 par. 1, n. 7, GDPR: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quella di interessato si ha all'art. 4, par. 1, n. 1, "una persona fisica identificata o identificabile" alla quale si riferiscono i dati.

[77] Di cui all'art. 20 GDPR.

[78] Tali diritti costituiscono piena attuazione dei principi contenuti nella Dichiarazione europea sui diritti e principi digitali.

[79] Il principio di limitazione della conservazione, di cui all'art. 5, par. 1, lett. e), GDPR impone che i dati personali siano «conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

players diversi dai grandi operatori commerciali in grado, come tali, di fissare le regole del gioco imponendo unilateralmente condizioni contrattuali inique[80].

Nello specifico, le grandi infrastrutture informatiche hanno il potere di imporre unilateralmente condizioni (per l'accesso ai dati) particolarmente restrittive o economicamente svantaggiose per le controparti interessate. Tali condotte, che si possono sostanziare in una formula di "prendere o lasciare"[81], rappresentano un grave *vulnus* per l'equilibrio contrattuale, rifrangendosi, al contempo, sul corretto funzionamento del mercato.

Pertanto, al fine di combattere questo genere di abuso di potere contrattuale, nei rapporti endoprofessionali (soprattutto a tutela delle microimprese, delle piccole imprese e delle medie imprese)[82], il DA introduce, all'art. 13, regole specifiche sulle clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo tra imprese. Tuttavia, non vi è alcuna preclusione applicativa e la previsione si applica quale che sia la dimensione dell'azienda, dunque, non solo nei rapporti *B2b*. Sono esclusi i rapporti con i consumatori (già regolati, sul punto, dalla direttiva 93/13/CEE): come è previsto nell'art. 1, par. 9, il DA "integra e fa salvo il diritto dell'Unione volto a promuovere gli interessi dei consumatori e a garantire un livello adeguato di protezione dei consumatori, nonché a proteggere la loro salute, la loro sicurezza, i loro interessi economici, in particolare le direttive 93/13/CEE, 2005/29/CE e 2011/83/UE".

La disposizione è volta a reprimere le condotte contrattuali abusive aventi ad oggetto l'accesso ai dati e il relativo utilizzo, indirizzando il comportamento delle parti verso una negoziazione svolta secondo buona fede e correttezza, introducendo termini e condizioni contrattuali ragionevoli, conformi alle buone prassi commerciali.

A titolo di chiarimento, il DA dispone che le clausole contrattuali che riproducono disposizioni obbligatorie dell'UE oppure disposizioni del diritto dell'UE che si applicherebbero se le clausole contrattuali non disciplinassero la materia non sono ritenute abusive (par. 2).

La previsione non è finalizzata a proteggere gli interessi economici nel contratto, *stricto sensu* intesi, ma è posta a presidio della libertà contrattuale; in ragione di ciò, essa non si applica alle clausole contrattuali che ne definiscono l'oggetto, né l'adeguatezza del prezzo rispetto ai dati forniti in cambio (par. 8).

Le clausole contrattuali abusive sono ritenute non vincolanti[83].

Sono definite tali, in generale, le clausole che si discostano "considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza" (par.

---

[80] Considerando 61. Si v. in argomento A. RICCI, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, cit., 808 e B. KARSTEN, *VII. Unfair Terms for Data Access and Use between Enterprises (Art. 13)*, in M. HENNEMANN, G.K. EBNER, B. KARSTEN, G. LIENEMANN, M. WIENROEDER (eds.), *Data Act. An introduction*, cit., 141 ss.

[81] Considerando 59.

[82] La definizione è contenuta nella raccomandazione della Commissione europea del 6 maggio 2003, n. 2003/361/CE.

[83] Il dibattito scientifico su questo ambito è molto vasto, si vedano, fra gli altri, V. ROPPO, *Regolazione del mercato e interessi di riferimento: dalla protezione del consumatore alla protezione del cliente*, in *Rivista di diritto privato*, 2010, 19 ss.; R. DI RAIMO, *Autonomia privata e dinamiche del consenso*, Napoli, 2003; sia consentito il rinvio a M.L. CHIARELLA, *Contrattazione asimmetrica. Segmenti normativi e costruzione unitaria*, Milano, 2016, 80 ss., 116 ss.

2). La disposizione, poi, distingue tra clausole abusive appartenenti alla lista nera (par. 4) e clausole, imposte unilateralmente, che invece "si presumono" tali e appartengono alla lista grigia (par. 5)[84], con possibilità per la parte contraente che ha inserito la clausola di provare che la medesima non è stata imposta unilateralmente (par. 6).

Si assiste sostanzialmente ad una dicotomia analoga a quella presente nella direttiva 93/13/CEE e caratterizzante la disciplina delle clausole abusive nei contratti con i consumatori. La presunzione di abusività, nella disciplina consumeristica, può essere superata dimostrando che la clausola è stata oggetto di trattativa individuale (art. 3 della Direttiva). Se in presenza di una posizione di forza o dominanza nel contratto, la libertà contrattuale della parte debole viene inibita, non potendo concorrere alla definizione del regolamento contrattuale, unilateralmente predisposto, la si potrà ripristinare con la richiesta di accertamento della vessatorietà della clausola finalizzata alla sua eliminazione dal contratto. La trattativa individuale, in particolare, non vale ad escludere la sussistenza di uno squilibrio nel contratto tra i diritti e gli obblighi delle parti, ma serve a dimostrare che esso non sia frutto di una imposizione da parte del professionista.

Nel testo dell'art. 13 non è prevista altra prova contraria a favore del predisponente, ciò nondimeno questa si trova nel Considerando 61: "l'impresa che impone la clausola contrattuale dovrebbe poter confutare la presunzione di abusività dimostrando che la clausola contrattuale inclusa nell'elenco del presente regolamento non è, nel caso di specie, abusiva".

Pertanto, dovrà essere effettuato un test di abusività della clausola unilateralmente imposta (come si legge nel Considerando 59), valutando se questa rientri nella previsione generale dell'art. 13, par. 3, in quella più particolare di cui ai par. 4 e 5 del DA, e debba essere considerata *sic et simpliciter* abusiva e, quindi, non vincolate[85] oppure in quella del par. 5 del medesimo articolo, che disciplina le ipotesi di presunta abusività, richiedendo un'indagine più approfondita. Secondo un repertorio già noto: la parte che ha imposto unilateralmente la clausola non potrà invocarne la natura abusiva (par. 6); l'invalidità che riguarda la singola clausola non investe l'intero contratto, allorché la clausola abusiva sia scindibile dalle altre (par. 7).

Il quadro di garanzie ora delineato è inoltre rafforzato dal diritto a un congruo compenso per le imprese per la messa a disposizione dei dati, che deve essere equo e non discriminatorio, nonché dalla previsione di adeguati meccanismi di risoluzione delle controversie[86].

Un ulteriore aspetto riguarda gli obblighi di condivisione e utilizzo dei dati detenuti dalle imprese, dagli enti pubblici e dalle istituzioni, agenzie o organismi dell'Unione (art. 14). Questa disposizione include certamente tutti quei casi in cui si verificano circostanze che giustificano un'eccezionale necessità di dati (art. 15). Si prevede, in particolare, di limitare con precisione le categorie dei casi di accesso a tali dati, imponendo specifici obblighi di motivazione nella richiesta di accesso da parte dei soggetti pubblici autorizzati (art. 17).

[84] Art. 13 DA.
[85] Si v. anche il considerando (58) DA.
[86] Art. 9 DA.

6. Conclusioni.

Il quadro delineato nel presente contributo descrive le modalità attuative di un importantissimo tassello della Strategia europea, che mira a creare equità nell'economia dei dati e consentirne la maggiore valorizzazione.

Attraverso la previsione delle strutture portanti necessarie, il DA rimuove le barriere giuridiche e strutturali che limitano la circolazione e rafforza percorsi, come nel caso delle regole in materia di interoperabilità di cui agli artt. 33 e ss., che ne agevolino la piena attuazione. I benefici che ne derivano si collocano a vantaggio non soltanto del DA medesimo, ma anche a beneficio delle altre normative che implicano il trattamento e una governance dei dati, come nel citato caso dell'AI ACT.

La piena efficacia di queste regole è però condizionata alla concreta attuazione delle disposizioni del regolamento stesso, soprattutto alla sua corretta implementazione ed alla piena applicazione da parte degli Stati membri. Al riguardo, un'armonizzazione "dal basso" da parte dei *market players,* mediante una diffusione di buone pratiche contrattuali di diffusione dei dati, presenta un'utilità imprescindibile[87], per quanto obiettivamente complessa.

Una particolare perplessità è legata al notevole investimento in termini tecnologici e di *compliance*, nonché al necessario perseguimento di un adeguato livello di competenze, per riuscire a garantire le nuove prescrizioni normative.

Ai destinatari del DA compete, pertanto, un importante impegno di natura pratica e sostanziale, per riuscire a stare al passo con ritmi tecnologici incessanti e sempre più esigenti[88].

Le perplessità più forti emergono dalla complessa articolazione normativa, che, vista la numerosa presenza di attori coinvolti, può presentare problematiche nella individuazione dei ruoli e dei rispettivi diritti.

Inoltre, la natura fortemente trasversale del DA comporta l'evidente opportunità di impostare una pianificazione di *compliance* che tenga conto di tutte le normative coinvolte e dei relativi adempimenti che ne derivano.

Da ciò consegue un'evidente onerosità di adeguamento, in ragione dei costi di *compliance*, della progettazione di piani di conformità, di costante revisione dei processi e dei piani infrastrutturali di raccolta e gestione dei dati, anche al fine di garantire la tutela dei segreti industriali[89] e il corretto interscambio dei dati.

In conclusione, si può affermare che gli avanzamenti tecnologici e, con essi, il potenziale economico che ruota attorno alla valorizzazione dei dati rendono il DA una punta di diamante della strategia economica europea. Il rischio da scongiurare è che il sistema normativo così impostato sia obiettivamente non attuabile dai destinatari, per le problematiche passate in rassegna.

Il quadro giuridico introdotto dal legislatore comunitario, complessivamente osservato nella strategia digitale ed economica europea, è caratterizzata da

[87] R. MONTINARO, *Responsible data sharing for AI: a test bench for EU Data Law*, in questa *Rivista*, 2024, 1, 1 ss.
[88] A. RICCI, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, cit., 824.
[89] In prospettiva critica, v. ancora la riflessione di G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., 990.

importanti obiettivi, per la cui efficacia occorrerà un grande impegno da parte di tutti gli Stati Membri[90] e degli attori coinvolti.

[90] Le perplessità implementative e la necessaria collaborazione degli Stati sono stati rilevati fin dai primi lavori preparatori del DA: si v., in tal senso, C. PERARNAUD, R. FANNI, *THE EU DATA ACT. Towards a new European data revolution?*, CEPS Policy Insights, n. 2022-05 / March 2022 (https://www.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-05_The-EU-Data-Act.pdf).