Accademia

Rivista dell'Associazione Civilisti Italiani

Direttore: ***Vincenzo Cuffaro***

numero sette Gennaio - Aprile 2025

Pacini Giuridica

Accademia
Rivista dell'Associazione Civilisti Italiani

I contributi sono sottoposti alla procedura di revisione anonima (*single blind peer review)* nel rispetto dei criteri indicati nel vigente Regolamento Anvur.

Iscrizione al R.O.C. n. 6269
Rivista online in open access periodicità quadrimestrale
ISSN 2974-8755

Direzione e Redazione:
Roma

Produzione e distribuzione
Pacini Editore srl – Via Gherardesca 1 – 56121 Pisa Ospedaletto – tel. 050 313011

Sommario

CONFRONTI

ORIENTAMENTI

OPINIONI

INTERSEZIONI

OSSERVATORI

Sommario

Guido Alpa aveva suggerito di aprire il primo numero del 2025 di *Accademia* con la segnalazione della ricorrenza dei venti anni del codice del consumo e la proposta era stata prontamente raccolta affidando a Liliana Rossi Carleo il festeggiamento dell'anniversario; il dialogo che veniva così instaurato appare ora velato di mestizia per la scomparsa di colui cui viene giustamente riconosciuta la paternità dell'importante testo normativo.
Il dialogo con gli amici scomparsi segna anche le pagine dedicate alla figura di Andrea Belvedere, cui la civilistica è debitrice di una preziosa lezione di metodo, come ben illustra la acuta riflessione di Aurelio Gentili sulla portata ed il valore teorico del metodo analitico-linguistico nel rapporto tra diritto e linguaggio.
Il diritto di matrice europea, a maggior ragione nel tempo presente, continua ad essere al centro dell'attenzione e ne offrono significativa testimonianza non solo le attente considerazioni che Carmelita Camardi, nella sezione **Confronti**, dedica ai modelli regolativi della responsabilità civile adottati nell'ordinamento europeo, ma anche le serrate analisi che, nella medesima sezione, Franco Trubiani e Edoardo Bacciardi – prendendo spunto dalla sentenza 14 novembre 2024, causa C-646/22 e riprendendo le fila di un dibattito avviato già nel primo numero di *Accademia* – svolgono sulla nozione di consumatore medio qual è delineata dalla giurisprudenza della Corte di giustizia. Alla giurisprudenza della CEDU ha invece riguardo lo scritto che, nella sezione **Orientamenti**, Marco Rizzuti dedica all'illustrazione di due decisioni nelle quali la Corte affronta il tema, suggestivo e ricco di reminiscenze storiche, del possibile pregiudizio dei diritti umani, nella specie prospettata con riferimento alla vita privata e familiare ed al pacifico godimento dei propri beni, derivante da una programmazione successoria adottata in base ad una legislazione aliena dal riconoscere i diritti dei legittimari. La risposta negativa offerta dalla Corte di Strasburgo vale così ad illuminare il tema della posizione dei legittimari nei singoli ordinamenti nazionali.
Sul medesimo tema possono leggersi, ancora nella sezione **Confronti**, i due aggiornati contributi che Cristiano Cicero e Gregorio Pacini dedicano al dibattito, ricorrente, di riforma della successione necessaria. In una

prospettiva in qualche modo limitrofa, Massimo D'Auria, nella sezione **Opinioni**, illustra invece i termini della questione che l'ordinanza della seconda sezione, 2 gennaio 2025, n. 23, ha proposto di rimettere all'esame delle Sezioni unite circa il possibile esperimento dell'azione surrogatoria da parte del creditore del legittimario pretermesso, per stabilire quale rilievo sia da attribuire all'inerzia del legittimario nell'esercizio dell'azione di riduzione.

In questo numero di *Accademia* sulla materia delle successioni a causa di morte si raccolgono dunque numerose analisi, ma non meno ricco è il versante degli studi dedicati alla responsabilità civile.

Al già ricordato saggio di Carmelita Camardi si aggiungono i contributi di Stefania Pia Perrino, Valentina Di Gregorio, Mirko Faccioli, e Roberto Carleo nei quali, con accenti diversi e da differenti prospettive, il tema è declinato con riferimento a specifici settori dell'esperienza giuridica.

La responsabilità delle strutture sanitarie, la responsabilità per illecito trattamento dei dati personali, la responsabilità del produttore di farmaci sono tutti ambiti nei quali il profilo dell'illecito assume valenze particolari, messe ben a fuoco nelle pagine dedicate all'analisi dei testi normativi e dei contributi giurisprudenziali.

Sul medesimo tema *Accademia,* fedele al programma di offrire al lettore un quadro aggiornato del dibattito anche internazionale, ospita nella sezione **Osservatori** l'interessante testo di Florence George che illustra la recente riforma del codice civile belga sulla responsabilità extracontrattuale.

Le Sezioni unite della cassazione saranno presto chiamate a pronunciare sulla questione di indubbio rilievo teorico (e non solo) della rinunzia alla proprietà immobiliare. La questione, ancora una volta posta direttamente da giudici di merito ai sensi dell'art. 363-*bis* c.p.c., tocca da vicino il 'terribile diritto': le **Opinioni** che Cesare Trapuzzano, Rolando Quadri e Giuseppe Guizzi sviluppano in un appassionato confronto consentono di valutare il profilo dogmatico e costituzionale dell'atto di rinunzia ed insieme di cogliere le matrici storiche e ideologiche che, sottese al principio della sovranità dello Stato sui beni rilasciati dal privato, rendono effettivamente discutibile la pretesa di sindacato sull'atto abdicativo.

Il medesimo fascino che accompagna il diritto di proprietà segna l'idea del potere, del quale a ben vedere la proprietà è appunto espressione nei rapporti privati. Questa concomitanza se non sovrapposizione di prospettive ha suggerito di anticipare alcune relazioni discusse in occasione del Convegno annuale dell'Associazione su 'Costituzione e diritto privato'.

Nella sezione **Intersezioni**, compaiono gli importanti interventi che Gaetano Silvestri, Maria Rosaria Ferrarese e Marco Ruotolo hanno dedicato agli aspetti pubblicistici della *governance*, alle metamorfosi del potere, sino al ruolo attuale da assegnare alla *Drittwirkug*, ponendo interrogativi cui sarebbe ingiustificato il rifiuto di rispondere da parte dei civilisti.

Buona lettura!

Circolazione dei dati e innovazione tecnologica

Valentina Di Gregorio
Prof. ass. Università di Genova

Sommario: 1. La regolamentazione dei dati nel mercato digitale. – **2.** Dalla *data protection* alla *data economy:* il *Data Governance Act*. – **3.** Verso uno spazio europeo dei dati: il *Data Act*. – **4.** Circolazione dei dati e intelligenza artificiale nel nuovo *AI Act*.

1. La regolamentazione dei dati nel mercato digitale

La rapidità dell'innovazione tecnologica, la digitalizzazione dei prodotti e dei servizi, lo sviluppo di un mercato sempre più competitivo nel campo della gestione e dello sfruttamento delle informazioni hanno accresciuto negli ultimi anni il valore potenziale dei dati per le imprese, i consumatori e più in generale per la società, contribuendo ad incentivare un processo economico nel quale ha assunto un ruolo primario l'intelligenza artificiale, scienza capace di generare dati e di amplificare gli effetti (positivi e negativi) derivanti dalla loro circolazione, agevolata dalla facilità di utilizzo delle piattaforme informatiche.

In questo contesto hanno svolto un ruolo fondamentale la scienza digitale e computazionale, la robotica, la bioingegneria, fondate su algoritmi e metodi di machine learning che raccolgono, analizzano ed elaborano e consentono alle digital companies di offrire prodotti e servizi di livello sempre più sofisticato e adattato alle esigenze della collettività[1].

[1] Il reg. (UE) 2024/1869 (Regolamento sull'intelligenza artificiale) del 13.6.2024, noto come *AI Act*, che stabilisce regole armonizzate sull'intelligenza artificiale, offre la prima definizione legislativa di un sistema di "AI" in termini di "*sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che puo presentare adattabilita dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti*, raccomandazioni o decisioni *che possono influenzare* ambienti *fisici o virtuali*". Il tema è attualmente oggetto di particolare attenzione da parte del la comunità scientifica e di numerosi scritti, tra cui, *ex multis*, Finocchiaro, *Diritto dell'intelli-*

L'interconnessione digitale, l'affermarsi della data economy, in cui il dato diviene l'oggetto degli scambi commerciali (data based) e non solo la sua fonte (data driven) e l'utilizzo dei sistemi di intelligenza artificiale, hanno conferito natura negoziale ai dati (anche personali) che possiedono nell'attuale momento storico anche un valore economico[2].

Le trasformazioni determinate dalle tecnologie basate sui dati e le ricadute in termini di vantaggi dell'uso delle informazioni che da essi possono trarsi sul piano economico e della crescita sostenibile per le imprese europee, hanno progressivamente condotto ad un cambiamento di approccio del legislatore europeo in materia di gestione dei dati, segnato dal passaggio dalla primazia della protezione consacrata nel reg. (UE) 2016/679 (GDPR) per i dati personali e nel reg. (UE) 2018/1807 per i dati non personali, alla valorizzazione dei dati "interoperabili" (personali e non personali) in un quadro di data sharing per fini "di sovranità tecnologica dell'Europa"[3], obiettivo principale dei recenti reg. (UE) 2022/868 (Data Governance Act, DGA) e reg. (UE) 2023/2854 (Data Act, DA)[4] che partecipano alla composizione del quadro regolatorio europeo in tema di dati[5].

---

genza artificiale, Bologna, 2024; Alpa, *L'intelligenza artificiale. Contesto giuridico*, Modena, 2021; Id. (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020; Ruffolo (a cura di), *Intelligenza artificiale - Il diritto, i diritti, l'etica*, Milano, 2020. Il fondamento di questa scienza è ricondotto agli studi di Alan Turing, considerato il padre dell'informatica (Turing, *Computing machinery and Intelligence*, in *Mind*, *New Series*, 1950, 59). Per una riflessione nel settore medico-sanitario v. D'Adda, *Danni « da robot» (specie in ambito sanitario) e pluralita di responsabili tra sistema della responsabilita civile ed iniziative di diritto europeo*, in *Riv. dir. civ.*, 2022, 805 ss. e Morley et al., *Governing Data and Artificial Intelligence for Health Care: Developing an International Understanding*, in *JMIR Form. Res*., 2022, vol. 6, 1 ss. Nel settore dei trasporti, soprattutto sotto il profilo economico: Servou et al., *Data, AI and governance in MaaS – Leading to sustainable mobility?*, in *Transportation Research Interdisciplinary Perspectives,* 19, 2023.

[2] Sul tema del dato come bene giuridico suscettibile di scambio v. Morace Pinelli, *Dalla* Data Protection *alla* Data Governance*: il regolamento UE 2022/*868, in *Nuova giur. civ. comm*., 2024, 487; Id., *Introduzione,* in *La circolazione dei dati personali*. *Persona, contratto e mercato*, Pisa, 2023, 2 e 16 ss.; Ainis, *Circolazione dei dati personali e disciplina del mercato,* ivi, 53 ss.; Ricciuto, *Il contratto e i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali,* in *Riv. dir. civ*., 2020, 642 ss. Sulle sfide della *data economy*, sotto l'angolo visuale specifico dell'AI, Nitzberg, Zysman, *Algorithms, data, and platforms: the diverse challenges of governing AI,* in *Journal of European Public Policy*, 2022, 1753 ss.

[3] Così la relazione della Commissione europea "*Una strategia europea per i dati*" (*https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_it*), in cui si precisa che la strategia europea è diretta a far acquisire all'Unione Europea una posizione di *leadership* nella società basata sui dati con la creazione di un mercato unico che consenta ai dati di circolare liberamente all'interno dell'UE e in tutti i settori a vantaggio delle imprese, dei ricercatori e delle pubbliche amministrazioni.

[4] Il reg. (UE) 2022/868 del 30.5.2022 relativo alla *Governance* europea dei dati precisa che "*gli ostacoli alla condivisione dei dati impediscono un'allocazione ottimale dei dati a vantaggio della società*" (cons. n. 2). Sul tema v. Bravo, *Intermediazione di dati personali e servizi di Data sharing dal GDPR al Data governance act*, in *Contr. e impr. Europa*, 2021, 199 ss. e, in particolare, sulla normativa introdotta con il reg. (UE) 2023/2854 (*Data Act*, DA) Ricci, *Introduzione al regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *Nuove leggi civ. comm*., 2024, 804.

[5] Per alcune illuminanti riflessioni sui rapporti tra diritto e tecnologia: Alpa, *opp. citt.,* Rodotà, *Tecnologie e diritti*, Bologna, 1995; Lipari, *Le categorie del diritto civile*, Milano, 2013.

Con una visione sovranazionale, la Commissione, consapevole degli ostacoli allo sviluppo dell'economia dei Paesi dell'Eurozona posti dalle limitazioni alla circolazione dei dati, si è prefissata il fine di rafforzare la competitività europea con l'istituzione di uno "spazio unico europeo dei dati" "senza frontiere", per garantire la disponibilità di un maggior numero di dati in Europa, "mantenendo al contempo al centro dell'attenzione le imprese e gli individui che generano i dati e che ne hanno il controllo", con l'intento di esercitare un ruolo chiave nello sviluppo e nel controllo della tecnologia[6].

Il metodo per generare ricchezza e apportare benefici nei vari settori, come quello sanitario, della mobilità, dei servizi pubblici e nei rapporti tra cittadini e istituzioni, consiste nell'indirizzare le imprese e il settore pubblico verso scelte strategiche efficienti capaci di creare valore per l'economia e la società attraverso lo sfruttamento e la condivisione tra settori e Stati membri dell'enorme potenziale insito nella massa di dati in circolazione immessi tramite prodotti e servizi, nel rispetto delle dinamiche concorrenziali.

Tutela dei dati personali e sviluppo del mercato europeo costituiscono già principi fondanti del GDPR ove la "libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali"[7] è sancita nell'art. 1 e traspare dall'obiettivo della creazione di uno spazio di libertà, sicurezza e giustizia, del rafforzamento delle economie nel mercato interno che presuppone la conciliazione tra protezione dei diritti delle persone fisiche e circolazione dei dati, rintracciabile sia nel preambolo (cons. n. 4) in cui si dichiara che la funzione sociale del diritto alla protezione dei dati deve essere contemperata con i diritti fondamentali, sia nella norma sulla data portability che attribuisce all'interessato il diritto di chiedere ad un titolare del trattamento di trasferire i propri dati personali ad un altro soggetto senza impedimenti (art. 20)[8].

È noto tuttavia come il GDPR, nella finalità di preservare i diritti delle persone fisiche, abbia imposto una serie di limitazioni alla circolazione che inevitabilmente attraggono anche dati che, se gestiti con adeguate misure di tutela dei diritti personali, potrebbero essere, di converso, molto utili o addirittura indispensabili allo sviluppo dell'economia e della ricerca.

L'ampio numero di atti europei emanati in ambito digitale ove ha trovato dimora il Data Governance Act e da ultimo anche il Data Act, il cui focus è centrato sull'accessibilità al valore rappresentato dai dati e sulla loro interoperabilità, intesa come "la capacità di due o più spazi di dati o reti di comunicazione, sistemi, prodotti connessi, applicazioni, servizi di trattamento di dati o componenti di scambiare e utilizzare dati per svolgere le

---

[6] V. la 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,* 19.2.2020 (*https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066)* e il cons. n. 3 DGA.

[7] Cons. nn. 6 e 9 GDPR.

[8] V. sul punto S. Troiano, *Il diritto alla portabilita* dei dati, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di Zorzi Galgano, Milano, 2019, 195 ss.

loro funzioni"[9], rappresenta la risposta dell'Unione all'esigenza di rilancio dell'economia tramite l'utilizzo dei dati e l'espressione di una precisa ambizione delle politiche europee di potenziamento della competitività delle imprese.

Ne recano testimonianza, oltre all'esplicita menzione di tale finalità nei testi legislativi citati, anche il lessico utilizzato nelle norme, da cui emerge come il "titolare dei dati " (e non il titolare del trattamento) corrisponda al soggetto che ha "il diritto o l'obbligo di utilizzare e mettere a disposizione dati " (art. 2, n. 13 Data Act) cui competono diritti e obblighi specifici, e il dato non sia più solo un'entità da proteggere, ma un bene giuridico al quale è assegnato un valore intrinseco e ascritto un potenziale economico da sfruttare in modo equo e trasparente, con i conseguenti effetti in ambito industriale, commerciale e sociale.

In questo scenario trovano spazio gli interventi normativi mirati a promuovere, sotto diversi profili, una crescita economica sostenibile e a rafforzare la posizione dell'UE nel mercato digitale e dell'ICT, rappresentati dalla direttiva 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale[10], dalle due direttive 2019/770/UE, sui contratti di fornitura di contenuto digitale e di servizi digitali e 2019/771/UE sulla vendita di beni che incorporano contenuti digitali o servizi digitali interconnessi, che hanno integrato il codice del consumo nel settore della tecnologia digitale, cui hanno fatto seguito, nel quadro dell'uso dei dati nei servizi digitali, il Digital Service Act (reg. UE 2022/2065, DSA) in tema di sviluppo dell'economia nell'ambito delle reti e dei servizi e il Digital Markets Act (reg. UE 2022/1925, DMA) in materia di piattaforme online e concorrenza, facenti parte del Digital Services Package, con cui è stata delineata la disciplina di intermediari e piattaforme informatiche ove circolano dati, con l'obiettivo principale di prevenire le attività illecite attraverso la creazione di un contesto equo e aperto per le piattaforme e di un mercato digitale competitivo per tutte le imprese digitali, in condizioni di parità, indipendentemente dalle loro dimensioni, nel rispetto dei diritti fondamentali delle persone cui i dati sono riferibili.

Gli obiettivi della strategia europea mirata al rilancio del mercato basato sulla data economy continuano ad animare anche i progetti di legge in itinere.

In campo finanziario, ad esempio, la proposta di regolamento FIDA (Financial Data Access), nel quadro di un sistema di open finance, si pone il fine di "migliorare i risultati economici per i clienti dei servizi finanziari (consumatori e imprese) e le imprese del settore finanziario promuovendo la trasformazione digitale e accelerando l'adozione di modelli aziendali basati sui dati nel settore finanziario", agevolando i consumatori nell'accesso ai dati finanziari per ottenere prodotti e servizi personalizzati con strumenti basati sui dati che li supportino nel prendere decisioni informate, nel confronto tra

---

[9] Dir. 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale, recepita con d. lgs. n. 177/2021, dir. 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale, recepita con d. lgs. n. 173/2021.

[10] Dir. 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale, recepita con d. lgs. n. 177/2021, dir. 2019/790/UE sul diritto d'autore e sui diritti connessi nel mercato unico digitale, recepita con d. lgs. n. 173/2021.

offerte in linea con le loro esigenze specifiche. La proposta intende favorire le imprese, in particolare le PMI, con conseguenti vantaggi sia per gli enti finanziari che potrebbero essere in grado di sfruttare appieno le tendenze della trasformazione digitale, sia per i prestatori di servizi che godrebbero di nuove opportunità commerciali nell'ambito dell'innovazione basata sui dati[11].

L'apparato regolatorio orizzontale delineato dall'UE, finalizzato ad incentivare l'innovazione tecnologica e l'utilizzo dei dati a vantaggio delle imprese e dei consumatori, ha dato origine ad una stratificazione normativa dettata dall'urgenza di contenere gli effetti imprevedibili di un fenomeno che nella data driven economy, nei big data, nell'intelligenza artificiale trova la sua fonte di ricchezza. I numerosi interventi legislativi dedicati al settore digitale sono stati dettati dall'esigenza di fornire strumenti per il migliore sfruttamento dei dati in campo industriale, nei trasporti, nella tutela dell'ambiente e per le necessità della vita quotidiana per le quali sono oggi fruibili dispositivi connessi alla rete di uso comune (Internet of Things o IoT) o applicazioni basate su sistemi algoritmici di facile accesso, come ChatGPT di OpenAI o come il nuovo DeepSeek AI cinese.

Ne è derivato "un sistema" basato su un ampio materiale normativo, rimesso alla razionalizzazione dell'interprete, in cui confluiscono principi di carattere generale e norme settoriali che rispondono all'esigenza di rilancio dell'economia tramite la circolazione dei dati e l'uso dell'intelligenza artificiale, espressione di una precisa ambizione delle politiche europee di potenziamento della competitività delle imprese europee e di cooperazione tra gli Stati membri.

2. Dalla *data protection* alla *data economy*: il *Data Governance Act*

Il primo passo verso il superamento della visione incentrata prevalentemente sulla protezione dei dati personali (nonostante il GDPR sia diretto anche a promuovere la circolazione) è compiuto nel 2022 dal Data Governance Act che si propone di realizzare "un mercato interno digitale senza frontiere e una società e un'economia dei dati antropocentriche, affidabili e sicure", di "migliorare le condizioni per la condivisione dei dati nel mercato interno, creando un quadro armonizzato per gli scambi di dati" (cons. n.3).

Creare un quadro armonizzato per gli scambi di dati, facilitare la cooperazione tra gli Stati membri e consentire ai titolari dei dati di valorizzare il proprio patrimonio informativo attraverso la condivisione di dati personali e non personali e agli utenti di mantenere il pieno controllo dei propri dati, rappresenta il fine dell'azione legislativa dell'UE, con il limite dell'uso improprio dei dati in violazione dei diritti fondamentali, del rispetto

[11] Proposta di regolamento relativa a un quadro per l'accesso ai dati finanziari, COM (2023) 360 final, 28.6.2023. Cfr. sull'argomento Stanzione, *Open banking, Open Finance e protezione dei dati personali*, in Falce e Morera (a cura di), *Dall'Open Banking all'Open Finance. Profili di diritto dell'economia*, Torino, 2024, 65 ss.

del diritto di proprietà intellettuale e alla libera concorrenza (cons. nn. 17-21 e art. 3, 1° comma, lett. c).

L'obiettivo è quello di sbloccare una massa di dati utili per lo sviluppo economico, garantendone la circolazione libera e sicura, mantenendo al contempo il controllo della pubblica sicurezza e dell'ordine pubblico nel rispetto dei diritti fondamentali.

È il legislatore europeo, nel preambolo del DGA, a sottolineare l'opportunità di un'interazione tra circolazione dei dati, suscettibili di essere pregiudicati da pratiche di sfruttamento e diffusione potenziate anche dal ricorso all'intelligenza artificiale – che sulla base dell'analisi dei big data permette di semplificare le operazioni e prendere decisioni strategiche informate – e sviluppo delle nuove tecnologie all'interno di uno spazio comune europeo, da intendersi come mercato interno nel quale i dati possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione.

Il DGA, dedicato alla governance degli spazi dati europei, si inquadra in una linea di intervento che in materia di dati è stata strutturata dall'UE sulla base di quattro pilastri, di cui il primo delinea un quadro normativo "integrato", diretto a garantire un migliore accesso e un uso più responsabile che ha trovato espressione nel Data Act, finalizzato a incentivare la disponibilità dei dati e del riutilizzo in un contesto di parità e con l'eliminazione degli ostacoli per i consumatori e le imprese nell'accesso ai dati generati soprattutto dai dispositivi dell'Internet of Things[12].

Gli altri pilastri sostengono l'azione dell'UE nel rafforzamento delle capacità di ospitare, elaborare e utilizzare i dati con la previsione della creazione di spazi europei comuni e di infrastrutture cloud interconnesse per superare gli ostacoli legali e tecnici al- la condivisione in Europa (così il secondo pilastro), nel potenziamento dell'empowerment delle persone fisiche che prevede l'adozione di misure di supporto per l'utilizzo dei dati generati dall'uso dei dispositivi informatici e la creazione di migliori opportunità nell'economia dei dati per le persone giuridiche e in particolare per le PMI (terzo pilastro) e nella promozione dello sviluppo di spazi di dati comuni europei in settori economici strategici e in altri ambiti di interesse pubblico (quarto pilastro).

Il regolamento, in una prospettiva trasformativa e dinamica dell'economia digitale, si prefigge di valorizzare il potenziale insito nei dati (personali e non personali) e garantisce l'accesso affidabile e non discriminatorio da parte di singoli utenti e imprese con l'introduzione di una disciplina sul riutilizzo dei dati pubblici, sui servizi di intermediazione di dati e sulla registrazione volontaria dei soggetti che raccolgono e trattano dati per

[12] Sfide e pilastri sono indicati nella Comunicazione della Commissione *"Una strategia europea per i dati"*, cit., par. nn.4 e 5. Cfr. il documento di lavoro della Commissione, "*Common European Data Spaces*", SWD (2022) 45 final, 23.2.2022. Si veda anche Curry, Scerri e Tuikka, *Data Spaces. Design, Deployment, and Future Directions*, New York, 2022, 1 ss., *https://doi.org/10.1007/978-3-030-98636-0_1*. In materia di dati sanitari lo spazio comune europeo dei dati dovrebbe essere istituito con l'*European Health Data Space*, oggetto della proposta di regolamento COM (2022) 197 final, 3.3.2022, approvata dal Parlamento europeo il 24.4.2024 e all'esame del Consiglio.

scopi altruistici, nella direzione indicata nel primo dei pilastri individuati dalla descritti dalla Commissione europea[13].

Questi strumenti dovrebbero funzionare per rendere i dati reperibili, accessibili, interoperabili e riutilizzabili («principi FAIR per i dati»), garantendo al contempo un elevato livello di cybersecurity[14].

Una concreta modalità di applicazione dei principi è rappresentata dalla figura dei "servizi di intermediazione dei dati", di cui l'art. 2 offre una definizione in termini di "servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali" e che rivestono particolare importanza nel settore in ragione del ruolo svolto nel mercato dai data brokers e della finalità dello scambio e della circolazione dei dati attraverso strumenti collaborativi nell'ambito della fornitura di servizi di condivisione.

In un'ottica di semplificazione delle formalità e di incremento della circolazione non è previsto per tali servizi un regime di autorizzazioni come nel GDPR, ma una procedura di notifica all'Autorità nazionale competente della sussistenza dei requisiti che assicurino un grado di sicurezza rigoroso (artt. 11 e 12) che dovrebbero garantire il ruolo neutrale (condizioni paritarie e oggettive) svolto dagli intermediari rispetto agli scambi da realizzare mediante una separazione, nell'economia dei dati, tra fornitura, intermediazione e utilizzo dei dati, favorendo l'interoperabilità, la circolazione di dati facilmente fruibili, il riutilizzo di un ampio numero di dati nella disponibilità della pubblica amministrazione, con il coinvolgimento nel processo anche delle PMI e delle start up[15].

Quest'ultimo obiettivo è realizzabile, secondo il legislatore europeo, anche attraverso strumenti "altruistici", con i quali apportare benefici (con un compenso che non vada oltre la compensazione dei costi sostenuti) al progresso della ricerca scientifica, al miglioramento dei servizi sanitari e della mobilità, alla lotta ai cambiamenti climatici, all'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche europee, al miglioramento della fornitura dei servizi pubblici, o delle politiche pubbliche[16].

---

[13] Lasciando impregiudicate le competenze degli Stati membri in materia di sicurezza pubblica, difesa e sicurezza nazionale. V. sul punto, l'art. 1 del *DGA* e il commento di Poletti, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies,* 2022, 1, 46 ss. La disciplina dell'altruismo dei dati (artt. 15, 16-25) rappresenta una novità rilevante soprattutto se utilizzata in campo medico per quanto riguarda la donazione dei dati medici. V. sul punto Krutzinna e Floridi, "*Ethical Medical Data Donation: A Pressing Issue*" in Krutzinna e Floridi (eds.), *The Ethics of Medical Data Donation,* Springer, New York, 2019.

[14] Cons. n. 2 DGA.

[15] Sul punto v. il cons. n. 27 DGA.

[16] Art. 2, n. 16 DGA. Per una riflessione sulla prevalenza della tutela dei diritti fondamentali garantita dal GDPR, significativa della rilevanza della persona e non tanto del dato, v. Resta, *La regolazione digitale nell'Unione europea. Pubblico, privato collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 971 ss.

I dati possono essere messi a disposizione su base volontaria anche da parte degli enti pubblici (art. 5) che hanno la facoltà di condividere alcune categorie di dati (art. 3) per il riutilizzo, purché essi siano anonimizzati (nel caso di dati personali) e modificati, aggregati o trattati con altri metodi di controllo se riguardano informazioni commerciali riservate, ivi compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale e messi a disposizione in conformità al principio open by design and by default[17]. Il riutilizzo dei dati detenuti dagli enti pubblici dovrebbe favorire la ricerca scientifica con l'adozione di processi armonizzati intesi a rendere i dati facilmente accessibili nell'interesse pubblico (cons. n. 16).

Il rilancio dell'economia digitale dell'Unione si fonda quindi anche sulla partecipazione degli enti pubblici riguardo ai quali, in particolare, il bilanciamento tra sviluppo del mercato e tutela dei diritti delle persone costituisce criterio di selezione dell'accesso e del riutilizzo dei dati nel rispetto delle norme sulla trasparenza amministrativa e all'interno del perimetro delineato dalla direttiva Open Data, già indirizzata alla disciplina della circolazione dei dati nel quadro del progressivo sviluppo della tecnologia basata anche sull'intelligenza artificiale[18].

Per perseguire gli obiettivi di cui si è detto sono previste nell'art. 10 tre tipologie di servizi di intermediazione: a) servizi tra titolari dei dati e potenziali utenti nell'ambito di servizi che comprendono scambi di dati, creazione di piattaforme o banche dati comuni oltre all'istituzione di un'infrastruttura per l'interconnessione tra questi soggetti, nell'obiettivo di ridurre i costi di transazione e facilitando i contatti tra utenti e fornitori, b) fornitori di servizi tra interessati che mettono a disposizione dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati che ricevono assistenza per l'esercizio dei diritti di cui al GDPR e che funzionano come mezzo di controllo dei singoli individui sui dati che li riguardano, sulla base di un rapporto fiduciario; c) cooperative di dati impegnate a rafforzare la posizione dei singoli attraverso un'attività di consulenza sulla condivisione e sull'utilizzo dei dati e fornire un'adeguata informazione sul tema, sia nei rapporti tra imprese che nei rapporti tra queste e i consumatori (definite nell'art. 1, n. 15).

Il contenuto dell'attività degli intermediari riguarda dunque l'utilizzo, il riutilizzo, lo scambio, la condivisione, lo sfruttamento dei dati (anche a titolo oneroso, v. l'art. 12 lett. b, riguardo alle condizioni per la fornitura di servizi di intermediazione e l'art. 20, per l'altruismo dei dati) tra i soggetti identificati nelle nuove figure del data holder e del data user (descritti nell'art. 2, nn. 8 e 9, che si aggiungono al data subject di cui al GDPR al

---

[17] Cons. nn. 9 e 45 e artt. 2, nn. 10 e 16 DGA.

[18] Dir. 2019/1024/UE, *Open Data*, recepita con d. lgs. n. 200/2021. Il cons. n. 13 della direttiva chiarisce in particolare che "*L'informazione del settore pubblico o le informazioni raccolte, prodotte, riprodotte e diffuse nell'ambito di un compito di servizio pubblico o di un servizio di interesse generale sono un'importante materia prima per i prodotti e i servizi imperniati sui contenuti digitali e diventeranno una risorsa contenutistica ancora più importante con lo sviluppo di tecnologie digitali avanzate, tra cui l'intelligenza artificiale, le tecnologie di registro distribuito e l'Internet delle cose*".

quale l'art. 2, n. 7 rinvia), che detengono i dati grazie al diritto alla portabilità (direttamente o da parte di altre società che li hanno acquisiti) e che agiscono sulla base di un rapporto contrattuale che può ricondursi allo schema dell'appalto di servizi o del mandato.

Il titolare dei dati si differenzia dal titolare del trattamento del GDPR (data controller) sia per la tipologia di dati, che nel DGA riguarda quelli personali e non personali, sia per il perimetro dei dati sui quali ha il diritto di operare: i titolari dei dati (data holders) sono le persone giuridiche, compresi gli enti pubblici e le organizzazioni internazionali o le persone fisiche che non coincidono con gli interessati rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, hanno il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli (art. 2, n. 8), mentre gli utenti dei dati (data users) sono le persone fisiche o giuridiche che hanno accesso legittimo a determinati dati personali o non personali e che hanno diritto, anche a norma del GDPR in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali.

L'introduzione delle categorie del data holder e del data user accanto al data subject, si è detto, ha suscitato dubbi sulla configurabilità del dato personale come oggetto del diritto di proprietà, che determinerebbe non solo un cambio di paradigma[19] rispetto alla disciplina sui dati personali, ma anche un pericolo per la mercificazione della persona[20]. Contro questo rischio sono individuate nel capo IV (art. 16) del DGA le "organizzazioni per l'altruismo dei dati riconosciute nell'UE" che dovrebbero favorire la circolazione mettendo a disposizione quantità considerevoli di dati pertinenti per sostenere obiettivi di interesse generale, svolgendo quindi un'attività che non sfrutta il profilo commerciale del dato, ma si basa su una logica solidaristica e sociale opposta a quella sottesa ad un modello di property rights, attestata anche dagli obblighi di trasparenza e di tutela dei diritti degli interessati e dei titolari dei dati previsti nel regolamento (artt. 20 e 21).

Che le politiche europee favoriscano un'attenuazione della visione personalistica del dato è conclusione confermata dal valore conferito all'utilizzo e al riutilizzo dei dati che si pone a base anche dell'uso dei sistemi di intelligenza artificiale, scienza alla quale l'Unione Europea attribuisce funzione di motore dell'economia nella competizione con le multinazionali, ma è evidente altresì che il grado di controllo sul dato e il livello di limitazione nella circolazione o il divieto di uso dipendono anche dalla natura personale o non personale del dato; in quest'ultimo caso, la circolazione dovrebbe essere favorita sul presupposto della sua utilità per la crescita delle imprese europee, compatibilmente con il diritto di proprietà intellettuale, elemento che non sempre è di agevole identificazione perché i dati possono circolare anche in modalità mista.

---

[19] Il tema, in rapporto ai dati personali, è diffusamente trattato da Bravo, *Intermediazione di dati personali e servizi di Data sharing dal GDPR al Data governance act*, cit. e Id., *Le cooperative di dati*, in *Contr. impr.*, 2023, 757.

[20] Così, Morace Pinelli, *Dalla* Data Protection *alla* Data Governance, cit., 491.

Tale ultima fase della produzione legislativa europea in materia digitale, costituita dalla normativa sui prodotti e i servizi digitali, sulla governance e circolazione dei dati, volta precipuamente a favorire lo scambio di dati soprattutto di natura industriale e commerciale, riveste inoltre particolare importanza anche per i dati detenuti a fini di ricerca scientifica (cons. n.16), rappresentando il consenso al riutilizzo un'opportunità per la condivisione delle informazioni per la tutela della salute e dell'ambiente. Anche in questo caso, la promozione della fiducia nell'economia dei dati si unisce necessariamente al controllo sui dati strategici e sensibili anche non personali, riguardanti non solo la salute pubblica, la sicurezza e l'ambiente, ma anche la protezione dei consumatori, la tutela dei diritti di proprietà intellettuale e dei segreti commerciali, essendo il principio ispiratore della disciplina sempre il favore e non il freno alla circolazione[21].

In un'ottica coerente con l'istituzione di un sistema di governo dei dati che si dirige sia verso la promozione dell'innovazione, sia verso la funzione sociale e solidaristica del la condivisione, espressa nelle disposizioni che trattano dell'altruismo dei dati, restano fermi i principi dettati nel GDPR in caso di eventuale conflitto tra tutela dei diritti della persona e ragioni economiche (cons. n. 4 DGA).

Il regolamento sulla governance integra dunque il quadro regolatorio europeo sui dati introducendo figure deputate alla gestione equa, affidabile e trasparente, fissando principi programmatici e istituendo meccanismi che garantiscono il controllo da parte degli interessati e dei titolari dei dati, benché non sia ancora chiaro come tali principi potranno trovare applicazione pratica.

Un'esplicazione, pur nel dubbio sulla raggiungibilità dell'obiettivo del controllo dei dati da parte degli utilizzatori dei prodotti e dei servizi, può trovarsi nel Data Act, dedicato a facilitare l'accesso e l'utilizzo dei dati da parte di imprese e consumatori per quanto riguarda la condivisione, la disponibilità e l'interoperabilità dei dati generati dall'uso di prodotti connessi e di servizi correlati alla rete e per incentivare le imprese a investire nel settore. In questo contesto anche le Authorities possono svolgere un determinante ruolo di controllo che non dovrebbe ostacolare le economie di mercato.

3. Verso uno spazio europeo dei dati: il *Data Act*

Le moderne economie digitali si basano ormai su dispositivi informatici, elettronici, multimediali connessi come i prodotti di domotica e gli elettrodomestici, gli assistenti virtuali, le smart cars, le macchine industriali, i droni, i device utilizzabili in healthcare, come smartwatch, wearable devices, dotati di sensori fisici che raccolgono segnali analogici (luce, suono, temperatura, movimento fisico) e li convertono in dati elettronici

[21] Shabani, *The date governance act ad the EU's move towards facilitating data sharing,* in *Molecular System Biology*, 2021, 17:e10229 e *https://doi.org/10.15252/msb.202110229*, rileva l'importanza di regole che favoriscano l'espressione di un consenso al riutilizzo di dati per scopi scientifici, anche tramite intermediari o organizzazioni con scopi altruistici.

binari, elaborati da un software incorporato o comunicati a server remoti per un'ulteriore elaborazione.

L'utilizzo di dispositivi collegati alla rete e la connessione con un servizio, attuata tramite applicazioni per l'utilizzo del prodotto, consentono al fornitore o al titolare dei dati di ricevere informazioni su tempi, modi e interazioni relative all'attività svolta con lo strumento utilizzato, sugli interessi dell'utente, sui contatti posti in essere con altri soggetti durante il servizio.

I produttori dei dispositivi, in questo campo, possono progettare strutture di dati c.d. "chiuse", in cui le misure di protezione tecnica a livello di hardware e software impediscono agli utenti del dispositivo di accedere direttamente ai dati solo sulla base delle condizioni contrattuali monopolistiche stabilite dai produttori o strutture c.d. "aperte", che al contrario, aumentano la concorrenza nei mercati dei dati a monte e nei mercati dei servizi basati sui dati.

Il GDPR, riguardo ai dati personali raccolti dai dispositivi digitali o dai servizi online, ha riconosciuto all'interessato persona fisica il diritto di accesso, di cancellazione e di portabilità dei dati personali e imposto l'obbligo per i responsabili del trattamento dei dati di ottenere il consenso degli interessati per la raccolta dei loro dati personali, ma l'accesso ai dati anche non personali e di dati pubblici raccolti ed elaborati per effetto di device elettronici connessi in rete (cui contribuisce anche l'intelligenza artificiale attraverso sistemi di Large Language Models), ha ricevuto considerazione solo nel Data Act che, come anticiipato, integra il precedente regolamento sulla governance attuandone i principi e che si propone di facilitare l'uso di un maggior numero di dati per imprese e consumatori, stabilendo norme armonizzate sull'accesso equo e age da parte degli utenti.

Nell'offrire nuove opportunità di utilizzare servizi basati sui dati[22] e un migliore accesso ai dati raccolti o prodotti da un dispositivo, con misure atte a ridurre i costi in caso di trasferimento dei dati a un altro fornitore di servizi cloud e a fornire garanzie contro i trasferimenti illeciti di dati, il regolamento appronta un sistema di condivisione dei dati collegati ai prodotti e ai servizi[23] – anche a titolo oneroso quando si tratti di rapporti tra imprese – tale da aumentarne la disponibilità, contribuendo alla realizzazione degli obiettivi di accrescimento della fiducia nei meccanismi volontari di condivisione dei dati[24].

---

[22] Il *Data Act* definisce, nell'art. 2. n. 1, i dati come "*qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi compilazione di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva*".

[23] I prodotti connessi e i servizi correlati nell'art. sono definiti nell'art. 2, nn. 5 e 6: i primi sono oggetti che possono generare, ottenere o raccogliere dati sull'uso, le prestazioni o l'ambiente in cui vengono utilizzati e che possono comunicare questi dati tramite connessione *wireless* o basata su cavo, mentre i servizi correlati sono servizi digitali che possono essere collegati al funzionamento di un prodotto connesso e che contribuiscono alla funzionalità di tale prodotto connesso trasmettendo dati o comandi.

[24] L'art. 3, n. 1 DA specifica "*in modo facile, sicuro, gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto*". Il compenso, per i rapporti tra imprese è previsto nell'art. 9.

Sono dunque previsti obblighi relativi ai rapporti tra imprese, tra consumatori o utenti e imprese e tra quest'ultime ed enti pubblici per l'accesso e l'utilizzo dei dati, allo scopo di ottimizzare i processi produttivi e migliorare i servizi offerti nella produzione di dispositivi tecnologici e macchinari industriali, anche con lo sfruttamento delle risorse proprie dell'intelligenza artificiale che, attraverso i dispositivi connessi e i servizi correlati ai prodotti utilizzabili (spesso in abbinamento) genera, a sua volta, una quantità di dati la cui qualità viene sottoposta ad una serie di procedure di controllo nel reg. (UE) 2024/1689 sull'intelligenza artificiale.

Se da un lato, tuttavia, l'eterogeneità e il volume delle informazioni accessibili, utilizzabili e trasferibili grazie allo sviluppo scientifico e tecnologico costituiscono "un'opportunità per l'innovazione e la competitività"[25] e uno strumento fondamentale per potenziare le risorse economiche delle imprese e accrescere la concorrenza con le grandi multinazionali con sede al di fuori dell'Europa, dall'altro, la circolazione dei dati, per rispondere alle esigenze dell'economia digitale, deve essere regolata, come già previsto nel DGA, tramite strumenti sempre più solidi di controllo dell'affidabilità che garantiscano l'interoperabilità a condizioni eque, ragionevoli, non discriminatorie e trasparenti[26] e che consentano il rispetto del segreto industriale sia nella fase della comunicazione dei dati, sia nella circolazione, tramite procedure di cybersecurity[27].

---

[25] Alcune critiche oltreoceano sono rivolte contro il favore che sarebbe riservato alle imprese UE: v. sul punto spec. Broadbent, *The EU Data Act, The long arm of european tech regulation continues,* in *Centre for strategic international studies*, *June* 2023, 1 ss, reperibile al link *https://www.csis.org/analysis/eu-data-act-long-arm-european-tech-regulation-continues*.

[26] Cons. n. 5 e art. 8 DA. L'art. 1, n. 3, del regolamento stabilisce l'applicabilità del regolamento ai fabbricanti di prodotti connessi immessi sul mercato dell'Unione europea e ai fornitori di servizi correlati, indipendentemente dal loro luogo di stabilimento, agli utenti nell'Unione europea di tali prodotti connessi o servizi correlati e ai titolari dei dati che mettono a disposizione dei destinatari i dati e a questi ultimi. Si applica agli enti pubblici, alla Commissione, alla Banca Centrale Europea e agli organismi dell'Unione che chiedono ai titolari dei dati di mettere i dati a loro disposizione, nel caso in cui tali dati siano necessari a fronte di una necessità eccezionale per l'esecuzione di un compito specifico svolto nell'interesse pubblico (come emergenze sanitarie o catastrofi naturali) e ai titolari dei dati che forniscono tali dati in risposta a tale richiesta, ai fornitori di servizi di trattamento dei dati, indipendentemente dal loro luogo di stabilimento, che forniscono i servizi a clienti nell'Unione europea ed ai partecipanti agli spazi di dati, ai venditori di applicazioni che utilizzano contratti intelligenti e alle persone la cui attività commerciale, imprenditoriale o professionale comporti l'implementazione di contratti intelligenti per altri nel contesto dell'esecuzione di un accordo.

[27] Da ultimo il reg. (UE, Euratom) 2023/2841 del 13.12.2023 che stabilisce misure per un livello comune elevato di cybersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione e la dir. (UE) 2022/2555, NIS 2, sulla sicurezza delle reti e delle informazioni) che prevede piani di sicurezza informatica individuali, una valutazione comune basata su criteri condivisi e standardizzati della solidità e dell'efficacia delle piattaforme, la revisione periodica e l'aggiornamento delle misure di protezione. Il *Data Act* distingue tra obblighi imposti ai produttori di *connected products* connessi nel mercato europeo e obblighi per i fornitori di *data processing services,* inclusi i servizi *cloud*, dettando norme armonizzate per rimuovere gli ostacoli alla circolazione dei dati e assicura-

Nel regolamento sono fissati principi in tema di condivisione dei dati da impresa a consumatore e da impresa a impresa, con l'obiettivo di renderli disponibili per una vasta platea di soggetti e con la previsione di un obbligo in tal senso in capo ai fornitori (venditore, locatore) verso gli utenti dei prodotti o dei servizi correlati, ai titolari dei dati, tenuti a mettere a disposizione dell'utente i dati nel caso in cui questi non possa accedere direttamente dal prodotto connesso o dal servizio correlato e con il riconoscimento del diritto degli utenti di condividere i dati con soggetti terzi (artt. 4 e 5). Nell'ambito delle relazioni tra imprese, i titolari dei dati che intendano mettere a disposizione i dati a titolo oneroso, sono tenuti a farlo a condizioni eque, ragionevoli, senza discriminazioni e in modo trasparente (art. 8).

La realizzazione di tale fine passa attraverso disposizioni dedicate alla disciplina del rapporto contrattuale tra le parti che si traducono nell'invito ad utilizzare clausole contrattuali tipo (non vincolanti), ad incentivare accordi di riservatezza, a rispettare protocolli di accesso rigorosi, norme tecniche, codici di condotta che consentono di preservare il segreto commerciale e ad inserire clausole contrattuali standard per agevolare le parti nella conclusione di contratti di cloud computing a condizioni eque, ragionevoli e non discriminatorie (art. 41)[28].

Il regolamento dedica una norma alle clausole abusive, identificandole nelle clausole contrattuali unilateralmente predisposte che limitano illegittimamente l'accesso e l'utilizzo dei dati, la responsabilità, il ricorso a mezzi di tutela contro la violazione degli obblighi relativi ai dati (art. 13) con l'effetto della nullità parziale (art. 13, 7° comma), simmetricamente a quanto previsto nel codice del consumo.

Le affinità con le clausole vessatorie del codice del consumo (art. 33) sfumano, tuttavia, con riferimento alla nozione di abusività che nel DA si caratterizza per essere "di natura tale che il suo utilizzo si discosta considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza" (art. 13, 3° comma), carattere che si estende alle condizioni in cui una parte, non avendo avuto alcuna possibilità di influenzare il contenuto del contratto rischia

---

re che i dati generati da un dispositivo connesso alla rete "*che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo*" (art. 2, n. 5) e da un servizio correlato, inteso come un "*servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto*" (art. 2, n. 6) e offerto insieme al prodotto o successivamente, "*siano accessibili all'utente in modo facile, sicuro, gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto*" (art. 3, n. 1).

[28] Art. 4, 6° comma. L'art. 41 prevede la stesura entro il 12.9.2025 di *"clausole contrattuali tipo non vincolanti relative all'accesso ai dati e al relativo utilizzo, comprese clausole su un compenso ragionevole e sulla protezione dei segreti commerciali, nonché clausole contrattuali standard, sempre non vincolanti, per i contratti di cloud computing, per assistere gli attori dello spazio digitale nella predisposizione di regolamenti contrattuali equi, ragionevoli e non discriminatori dal punto di vista dei diritti e degli obblighi contrattuali".*

di subire uno squilibrio di potere (art. 13, 6° comma), alle condizioni di provenienza unilaterale (art. 13, 1° comma), nonché alle clausole che direttamente o indirettamente sono rivolte a precludere l'applicazione delle norme del regolamento (art. 13, 2° comma). Il 4° comma dell'art. 13 prevede una tipizzazione delle clausole aventi natura di abusività con una esplicita presunzione in tal senso nel 5° comma. Inoltre, data la particolare importanza attribuita al diritto dell'utente di cambiare il fornitore del servizio, nelle disposizioni di cui al capo VI sul passaggio tra servizi di trattamento dei dati (definiti nell'art. 2 n. 8) sono imposti ai fornitori obblighi di informazione, di rispetto della clausola di buona fede nel processo di passaggio (artt. 26 e 27), di redazione di specifici contenuti contrattuali sui diritti del cliente nell'accordo tra le parti che deve rivestire forma scritta (art. 25), mentre altre disposizioni nel capo VIII impongono requisiti essenziali e regole molto dettagliate per consentire l'interoperabilità dei dati, dei meccanismi e dei servizi di condivisione nello spazio comune europeo.

La disciplina dovrebbe teoricamente rafforzare i diritti degli utenti, ma nonostante le previsioni astratte, restano dubbi sull'efficacia delle misure previste nell'uso di dispositivi IoT rispetto all'obiettivo di assicurare un controllo su profili che, diversamente da quanto accade più in generale nell'ambito dei rapporti B2C, sconta l'inadeguatezza delle conoscenze degli utilizzatori in campo tecnologico e di mercato digitale, la difficoltà nell'individuazione di carenze tecniche del servizio o di interoperabilità dei dati, dei meccanismi e dei servizi di condivisione a fronte del potere commerciale delle grandi imprese che predispongono le condizioni generali di contratto.

Una novità è costituita dall'art. 36 del regolamento che prende atto della rilevanza della figura degli smart contracts per l'esecuzione degli accordi di condivisione dei dati, offrendone una definizione nel precedente art. 2, n. 39 in termini di "programma informatico utilizzato per l'esecuzione automatica di un accordo o di parte di esso utilizzando una sequenza di registrazioni elettroniche di dati e garantendone l'integrità e l'accuratezza del loro ordine cronologico". Il vantaggio del ricorso ai contratti intelligenti è la riduzione dei costi[29] e lo sfruttamento dell'opportunità di usare tali contratti quali misure tecniche di protezione per impedire l'accesso non autorizzato ai dati e ai metadati, per mantenere il contratto sull'utilizzo e la messa a disposizione del prodotto o del servizio, sulla condivisione con terzi o sulla divulgazione dei dati da parte dei destinatari, nel rispetto delle disposizioni degli artt. 4, 5, 6, 8, 9 (così, l'art. 11).

L'attenzione alla tutela degli utenti emerge dalla prescrizione, nell'utilizzo di tali contratti, del rispetto di requisiti che devono risultare da una certificazione ottenuta a seguito di conformity assessment sul piano della robustezza e controllo dell'accesso, dalla previsione di meccanismi di cessazione e interruzione sicure del rapporto e di un

[29] V. sul tema diffusamente Maugeri, *Smart contracts e disciplina dei contratti*, Bologna, 2021 ed anche: Verstappen, *Legal Agreements on Smart Contract Platforms in European Systems of Private Law,* 1st ed., Springer, 2023; Corrales, Fenwick, Haapio, *Legal tech, Smart contracts and Blockchain*, Springer, 2019.

sistema di archiviazione dei dati, nonché dall'esigenza di coerenza con le clausole dell'accordo di condivisione dei dati che il contratto esegue. La disposizione contempla una presunzione relativa di conformità per i contratti intelligenti che soddisfano le norme armonizzate (4° comma) e le specifiche comuni (9° comma).

Le norme sugli smart contracts si applicano a qualsiasi accordo di condivisione dei dati, non solo quelli tra titolari e destinatari. Ciò significa che anche l'industria delle blockchain, che fa largo uso di tali contratti, dovrà conformarsi al regolamento se gli accordi sottostanti mirano alla "condivisione dei dati", benché il cons. n. 6 del regolamento, nel prevedere "norme orizzontali", consenta tanto all'Unione Europea, quanto agli ordinamenti nazionali di "affrontare le situazioni specifiche dei settori pertinenti".

Trattandosi di una normativa di recente introduzione non è possibile stimare quali saranno gli effetti concreti della sua applicazione, pur intravedendosi, nel quadro dei vantaggi derivanti dall'accesso a una massa di dati detenuti in modo esclusivo dai fornitori (e dai titolari del trattamento) dei prodotti e dei servizi, qualche dubbio di compatibilità tra interesse economico e pubblico alla condivisione dei dati e tutela dei diritti di proprietà intellettuale e della privacy, con possibile squilibrio delle posizioni a vantaggio di logiche concorrenziali.

Nell'armonizzazione dell'accesso ai dati su scala europea, che nasce anche dall'esigenza di ordine politico di sottrarre la dipendenza dell'Unione europea dalle multinazionali extraeuropee e di ridefinire i confini della sovranità digitale, si deve infatti tenere conto dei rischi di diffusione non autorizzata di dati insiti nelle informazioni generate da dispositivi connessi (come smartphone, elettrodomestici e sensori IoT) che potrebbero violare segreti industriali o diritti della personalità, infrangendo i sistemi di tutela approntati dagli ordinamenti. Ciononostante, non pare che il nuovo apparato regolatorio possa integrare un pericolo, emergendo chiaramente dal regolamento come la realizzazione dell'obiettivo dell'innovazione data driven, l'accessibilità e il controllo per consumatori e aziende sui dati che creano e la prevenzione di abusi di posizione dominante sia stata costruita su regole chiare per la condivisione dei dati, coerenti con le prescrizioni sull'utilizzo ottimale delle tecniche che consentono l'analisi di banche dati contenenti dati personali (quali l'anonimizzazione, la privacy differenziale, la generalizzazione, la soppressione e la casualizzazione, l'utilizzo di dati sintetici o metodi analoghi, nonché altri metodi all'avanguardia di tutela della vita privata, v. cons. n. 7) cui si uniscono valutazioni di impatto e altre tutela che contribuiscono a assicurare il rispetto di requisiti di sicurezza.

4. Circolazione dei dati e intelligenza artificiale nel nuovo *AI Act*

La grande massa di dati di cui oggi si può disporre per effetto dell'uso di motori di ricerca, di social network, di prodotti e servizi connessi alla rete ne ha potenziato il valore come risorsa della digital economy.

Poiché i dati costituiscono la base dell'intelligenza artificiale, vantaggi e rischi derivanti dalla disponibilità dei dati in circolazione sono illustrati nell'AI Act che, nell'inten-

to di delimitare i rischi derivanti dall'uso di processi decisionali automatici, analogamente a quanto previsto anche negli altri atti normativi cui si è trattato, mira a promuovere l'innovazione, ma al contempo a garantire il rispetto dei diritti fondamentali, fissando una disciplina per i sistemi algoritmici secondo principi di trustworthy AI e proteggendo salute, sicurezza, diritti fondamentali delle persone, democrazia, Stato di diritto, ambiente (art. 1)[30].

La preoccupazione di mantenere un equilibrio tra sviluppo della tecnologia e tutela dei diritti fondamentali è presente anche nella Convenzione recentemente approvata dal Consiglio d'Europa in tema di Artificial Intelligence and Human Rights, Democracy and the Rule of Law che ribadisce l'importanza dei requisiti di trasparenza, affidabilità, innovatività dei principi dei sistemi di intelligenza artificiale, con particolare attenzione ai principi di accountability, alla protezione della privacy e ai valori della democrazia[31].

La struttura del regolamento (UE) 2024/1869, costituita da un ampio articolato dedicato alla classificazione dei sistemi di intelligenza artificiale, alla definizione delle modalità di valutazione della conformità di tali sistemi alle prescrizioni legislative e alla disciplina degli organi di supervisione e controllo, meriterebbe un'ampia analisi non solo per le ricadute sul piano degli obblighi imposti alle imprese, ma anche nella prospettiva dell'inquadramento delle disposizioni contenute nello schema regolatorio nelle categorie giuridiche privatistiche, che in questa sede non si svolgerà compiutamente, limitandosi invece a qualche considerazione sui rapporti tra la diffusione di un fenomeno che di dati si nutre, oggi facilmente fruibile per tutti, e la regolamentazione ad essi riservata nei più recenti atti normativi europei.

Nell'evolversi della tendenza dapprima espressa in termini di diffidenza nei confronti delle potenzialità dell'informatica e dei suoi sviluppi per le minacce sul piano della violazione dei diritti delle persone e per la sicurezza, l'AI Act si pone come elemento costitutivo di un programma destinato a favorire lo sviluppo del mercato e incentrato sull'adozione di un approccio, tipico delle scelte di politica industriale, fondato sul rischio e su

---

[30] L'intelligenza artificiale "affidabile" è fondata sui principi della supervisione umana, della robustezza e della sicurezza degli algoritmi, della trasparenza, intesa come tracciabilità dei sistemi, della non discriminazione, della tutela del benessere sociale e ambientale, della responsabilità e del rispetto dei diritti fondamentali dell'individuo, della riservatezza dei dati personali.

[31] La Convenzione è stata sottoscritta il 5.9.2024 dal Consiglio d'Europa (*Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*) (https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence. Il regolamento è stato preceduto da una serie di atti resi sul tema a partire dal 2017, come la risoluzione del Parlamento europeo del 20.10.2020 sugli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)) (P9_TA(2020)0275), dalla risoluzione del Parlamento europeo del 20.10.2020 sul regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), dalla risoluzione del Parlamento europeo del 12.2.2019 sulla politica industriale europea in materia di robotica e intelligenza artificiale (2018/2088(INI) e dalla proposta di regolamento del Parlamento europeo e del Consiglio in materia di armonizzazione delle regole sull'intelligenza artificiale del 21.4.2021.

un modello che ne incentiva l'utilizzo purché nel rispetto di una serie di prescrizioni di conformità (nell'art. 3, n. 2, il rischio è definito in termini generali come una "combinazione di probabilità del verificarsi del danno e della sua gravità").

Lo spirito della disciplina è quello di favorire, con un approccio normativo orizzontale e non indirizzato a singoli settori, lo sviluppo e l'uso delle nuove tecnologie basate sull'intelligenza artificiale con regole che possono trovare applicazione in diversi ambiti, come quello sanitario, dei contratti, dei trasporti, della Pubblica Amministrazione ed anche nel campo della giustizia.

Nel promuovere una AI antropocentrica e affidabile, il regolamento prevede quindi una classificazione dei rischi e obblighi diversificati che devono essere osservati al momento della realizzazione del sistema, variabili in base al livello di rischio che ciascuna delle categorie delineate può determinare nei vari settori di applicazione (ad esempio salute o trasporti) con riguardo alla violazione dei diritti e delle libertà degli individui. La ratio è quella di non precludere, ma di incentivare lo sviluppo e l'uso dell'AI, sulla base dell'accettazione del rischio immesso allo scopo di favorire l'attività imprenditoriale e gli investimenti nel settore, con la prescrizione di obblighi alle imprese europee ed extraeuropee di conformità (v. art. 2), dettate anche in altre norme armonizzate, in contrapposizione alla logica sottesa al GDPR che, pur nella declamazione del favore per la circolazione dei dati, è soprattutto mirato alla protezione dei dati personali.

In base alla suddetta classificazione è possibile inquadrare le attività che prevedono l'uso dei dati tramite sistemi di intelligenza artificiale e stabilire conseguentemente gli obblighi che dall'appartenenza ad una determinata categoria incombono sui soggetti coinvolti (indicati nell'art. 2). Pertanto, fatta eccezione per le pratiche di AI vietate, indicate nell'art. 5, dalle quali può scaturire un rischio inaccettabile per la sicurezza, la salute o i diritti fondamentali delle persone, la cui tutela costituisce obiettivo del regolamento insieme al miglioramento del funzionamento del mercato interno (così, l'art. 1), la disciplina introdotta stabilisce una gradazione dei sistemi di AI da un rischio alto ad un rischio minimo, con una supervisione accurata, con specifici assessment necessari a garantire la conformità dei sistemi alle regole e un costante richiamo ai diritti fondamentali per i sistemi ad alto rischio, vale a dire per quei sistemi che presentano un alto potenziale di rischio di violazione dei diritti e che sono elencati, secondo un criterio di tipicità, nell'allegato I, ove è riportata la normativa di armonizzazione dell'Unione e nell'allegato III, con possibilità di estensione ad altre situazioni per opera della Commissione (ai sensi dell'art. 7)[32].

[32] L'art. 2 dell'*AI Act* richiama: *providers* di sistemi di AI o i modelli di AI per finalità generali immessi sul mercato o messi in servizio nell'UE, indipendentemente dal fatto che siano stabiliti o ubicati in UE o Paesi terzi; *deployers* (utilizzatori primari) interni all'UE; *providers* o *deployers* con stabilimenti in Paesi terzi laddove l'*output* prodotto dal sistema di AI è utilizzato all'interno dell'Unione; importatori e distributori di sistemi di AI; fabbricanti di prodotti che immettono sistemi di AI insieme al prodotto con nome e marchio; rappresentanti autorizzati di *providers*, persone interessate che si trovano nell'UE. Riguardo alle pratiche vietate, il 2.2.2025 sono entrate in vigore le linee guida

Il rischio basso riguarda invece una categoria di sistemi per i quali sono previsti specifici obblighi di trasparenza e informazione (art. 50): si tratta dei sistemi che interagiscono con le persone fisiche e che devono essere progettati e sviluppati per fornire adeguate informazioni su tale interazione. Se i dati sono utilizzati per generare contenuti audio, immagini, video (compreso il caso di deep fake), testi sintetici, è necessario che gli output del sistema siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente con soluzioni tecniche efficaci, interoperabili, solide e affidabili.

Se è presente nel sistema un meccanismo che permette il collegamento a dati personali, come il riconoscimento delle emozioni o la categorizzazione biometrica da cui scaturiscono informazioni riguardanti una persona fisica identificata o identificabile, al dovere di informazione si aggiunge l'osservanza delle regole contenute nel regolamento sulla protezione dei dati personali (v. art. 4, n. 1 GDPR).

Altre norme regolano le procedure di valutazione di impatto ai fini dell'individuazione del livello di rischio immesso in rete dal sistema. Tra queste il FRIA, fundamental rights impact assessment che controlla l'impatto sui diritti fondamentali (art. 27) e il conformity assessment (art. 43) che prevede anche l'adozione di standard specifici (art. 40) i quali, tuttavia, appaiono di difficile applicazione qualora si debba procedere ad una valutazione dell'impatto sui diritti fondamentali, non essendo chiaro come possa essere declinata una gradazione degli effetti su tali diritti.

Poiché, come si è detto, sono i dati ad alimentare l'AI, è la qualità dei dati e non tanto la quantità a giocare un ruolo nel quadro della valutazione del rischio insito nell'algoritmo. Nel regolamento si legge che "dati di alta qualità e l'accesso a dati di alta qualità svolgono un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione" (cons. n. 67). Di qualità dei dati tratta anche il GDPR nell'art. 5, secondo cui il titolare del trattamento è tenuto a garantire che i dati trattati siano adeguati, pertinenti e limitati alle finalità, esatti e aggiornati e a adottare misure ragionevoli per la cancellazione, la rettifica, l'archiviazione. Il trattamento dei dati personali con algoritmi, quindi, è ammissibile nel rispetto delle regole stabilite dal GDPR la cui applicazione, per espressa previsione dell'art. 2 n. 7, resta sempre prioritaria, come anche nel caso degli altri regolamenti fin qui esaminati.

Tuttavia, nel caso di categorie particolari di dati (quelle di cui all'art. 9 GDPR), il trattamento rientra nell'ambito dei sistemi ad alto rischio (art. 7, n. 2, lett. c), per i quali è stata dettata una norma specifica, l'art. 10 (Dati e governance dei dati), che riguarda tutti i tipi di dati, personali e non personali; poiché i sistemi algoritmici processano i dati con meccanismi di self learning, sono stabilite alcune procedure di controllo dirette a conte-

---

della Commissione Europea riguardanti le pratiche ritenute inaccettabili in quanto fonte di potenziali rischi per i diritti fondamentali, reperibili al link: *https://digital-strategy.ec.europa.eu/it/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act*.

nere il rischio che all'interno della mole di dati elaborati ne vengano trattati anche alcuni per i quali non è stata rispettata la base giuridica del GDPR (nel caso di dati personali) o che non sono affidabili (anche nel caso di dati non personali) perché privi dei requisiti che la stessa norma indica.

In particolare, è necessario che l'addestramento del modello di AI sia sviluppato sulla base di set di dati di training, convalida e prova conformi ai requisiti richiesti sul processo di raccolta, sull'origine (e sulla finalità nel caso di dati personali), sull'adeguatezza dei dati, sulle operazioni di trattamento pertinenti ai fini della relativa preparazione, come annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione, sulla valutazione presuntiva delle informazioni che i dati devono misurare nel processo di elaborazione, la loro adeguatezza, quantità e qualità, sull'esistenza di possibili distorsioni (bias), di lacune o discriminazioni che potrebbero inficiare l'affidabilità e la sicurezza del sistema, comportando il rischio della violazione dei principi che costituiscono il fondamento dell'impianto regolatorio costruito con gli ultimi atti normativi dell'UE[33].

L'applicazione del processo decisionale può infatti dare origine a distorsioni involontarie derivanti dalla progettazione e dall'impiego di un algoritmo soprattutto se riguardanti comunità di persone sottorappresentate, appartenenti ad una certa etnia, con disabilità, in campo sanitario o bancario; la presenza di bias nei progetti e nei dati di addestramento dell'algoritmo è in grado di alimentare le disuguaglianze esistenti tra persone e incoraggiare una distopia che il regolamento si è prefissato di evitare.

Sempre nella prospettiva dell'affidabilità del set di dati per l'addestramento dei modelli, l'art. 5, 3° comma richiede che i dati siano sufficientemente rappresentativi e "nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista", requisito quest'ultimo che suscita qualche perplessità, non potendo facilmente darsi garanzia dell'assenza di errori se non nella misura in cui si tratti di qualità del dato nel senso sopra descritto.

Considerata l'alta potenzialità delle piattaforme online di raccolta dei dati personali da siti (pubblici e privati) conferiti dagli interessati per specifiche finalità, si può ritenere che il rischio di un trattamento al di fuori del controllo imposto dal GDPR sia alto, sicché nel caso in cui, per la valutazione di eventuali distorsioni o discriminazioni, si renda necessario e indispensabile trattare dati personali, l'art. 10, 5° comma fissa specifici obblighi di protezione e sicurezza mirati a prevenire abusi, accesso a dati o trasferimenti non autorizzati riconfermando l'applicazione delle disposizioni del GDPR – e della dir. (UE) 2016/680, del reg. (UE) 2018/1725 –, con la previsione dell'obbligo di cancellazione dei dati dopo l'adozione della misura.

Le regole suddette valgono anche per i modelli di GPAI (General-purpose AI models) conosciuti anche come AI generativa, processo che utilizza i dati per elaborare nuo-

---

[33] Il controllo dell'affidabilità dei dati è principio espresso nei considerando dell'*AI Act* (cons.n. 1, 6), del DGA (cons. n. 3) e del DA (cons. n. 30) secondo il quale, in particolare, *"i titolari dei dati dovrebbero garantire che i dati messi a disposizione del terzo siano tanto accurati, completi, affidabili, pertinenti e aggiornati quanto i dati ai quali il titolare stesso puo essere in grado o avere il diritto di accedere in virtù dell'uso del prodotto connesso o del servizio correlato"*.

vi contenuti sfruttando le informazioni immesse in rete tramite l'uso di applicazioni o device (anche dallo stesso utente)[34], oggi fonte di incertezze e diffidenza – come è emerso anche dagli interventi e dalle decisioni del Garante italiano della privacy – per la difficoltà di accertamento dei requisiti sopra descritti e per i rischi di perdita di controllo sui dati (anche personali) trasmessi[35].

L'art. 53 (Obligations for providers of general-purpose AI models) prevede quindi, sotto questo profilo, ulteriori adempimenti anche di tipo documentale che attestino i caratteri del modello, il processo di training, di convalida e di prova, impone il rispetto di obblighi di accountability, di trasparenza, di informazione per i fornitori che intendono integrare nei loro sistemi il modello di AI c.d. "per finalità generali", prescrive la stesura di un elenco pubblico dei modelli GPAI caratterizzati da rischio sistemico (art. 52) e il rispetto della normativa sul diritto d'autore e sulla protezione dei dati personali, con l'eccezione dei modelli a licenza libera e open source in cui i parametri devono essere resi pubblici.

Per i modelli di AI generativa che presentano una capacità di impatto elevato, individuati anche con il ricorso ad un criterio quantitativo (art. 51, n. 2), l'art. 51 introduce la categoria dei sistemi a "rischio sistemico", assoggettati ad ulteriori processi di valutazione della conformità e del livello di rischio immesso, con protocolli e strumenti standardizzati (anche con adversarial testing), in cui è compresa la valutazione delle conseguenze delle decisioni, la registrazione degli incidenti gravi, la garanzia di un livello adeguato di cybersicurezza, la redazione di Codes of practice (art. 51).

Algoritmi, dati, potenza di elaborazione e piattaforme digitali (intese sia come attori del mercato e della società, sia come tecnologia) che generano i pool di big data su cui operano gli strumenti di cui si è detto costituiscono il terreno di interazione tra regolamenti sui dati e regolamento sull'intelligenza artificiale[36]. Pur essendo la normativa det-

---

[34] A proposito delle applicazioni della *Gen AI*, v., tra gli altri, Botunac et al., *Opportunities of Gen AI in the Banking Industry with regards to the AI Act, GDPR, Data Act and DORA*, in *13th Mediterranean conference on embedded computing* (MECO), 11-14 June 2024, Budva, Montenegro. Le tecniche di *machine learning* sfruttano una grande massa di dati per il loro funzionamento e *i Large Language Models* vengono addestrati su enormi *dataset* di testo che permettono di svolgere attività quali *text analysis*, *sentiment analysis*, traduzione e riconoscimento vocale. Il modello, tuttavia, non "memorizza" i dati in modo diretto, ma piuttosto, costruisce rappresentazioni statistiche e relazionali delle informazioni generando risposte plausibili basate su schemi appresi, senza avere accesso diretto ai dati originali. Oltre all'addestramento, i modi chiave di interazione tra i GPAI e i dati sono rappresentati dalla generazione di contenuti, come testi, immagini o musica, basati sulle conoscenze apprese dai dati di addestramento con la conseguente capacità di combinare e rielaborare informazioni in modi creativi. I GPAI possono raccogliere e analizzare dati in tempo reale dalle interazioni con gli utenti, sia per adattare le risposte e migliorare l'esperienza con l'utente, sia per migliorare le prestazioni nel tempo dei modelli con l'aggiornamento della piattaforma. In entrambi occorre esercitare un controllo nella condivisione dei dati anche con garantire meccanismi di *feedback*.

[35] Provv. Garante Privacy italiano n. 112 del 30.3.2023.

[36] Sui rapporti tra il *Data Act* e le altre normative europee rilevanti v., tra gli altri, Fernandez, *The Data Act: The next Step in Moving Forward to a European Data Space*, in *Eur. Data Prot. L. Rev.*, 2022, 108 ss., spec. 111.

tata nel regolamento frutto di un indirizzo strategico in tema di società digitale iniziato con lo sviluppo dell'ICT e di Internet, progredito con la data economy e pervenuto oggi, dopo una serie risoluzioni rese sui profili giuridici ed etici dell'AI, alla creazione di un apparato regolatorio ad ampio raggio con l'obiettivo di affermare l'Europa come leader nel settore (art. 1 AI Act), si deve rilevare come appaia al momento incerta la capacità del regolamento di controllare i dati generati dagli algoritmi e circolanti tramite piattaforme all'interno di una società globalizzata dove i dati non viaggiano isolati, ma come parte di una massa, frutto di diverse elaborazioni e sulla quale coesistono più trattamenti. Inoltre, l'approccio risk-based, se si mostra coerente con l'intento di permettere quanto più possibile il rilancio delle imprese, descrive norme programmatiche che non sempre sono sufficienti ad esonerare da responsabilità chi si occupa dello sviluppo del software o valuta la categoria di rischio, adottando le misure prescritte atte a rimuoverlo senza poter contare su metodi di eliminazione del rischio residuo, con la conseguenza dell'incertezza sul controllo dei dati.

Resta aperta la questione dell'individuazione del regime di responsabilità per danni derivanti dall'uso dell'AI, rimesso attualmente alla legislazione di ciascun Paese[37]. Sotto quest'ultimo profilo, la proposta di direttiva sul tema della responsabilità civile all'esame delle istituzioni europee delinea un regime piuttosto complesso, sia sotto il profilo della formulazione delle norme, in cui sono presenti rinvii e eccezioni che non ne facilitano la lettura, sia sotto il profilo sostanziale, soprattutto con riguardo alla scelta del ricorso ad un sistema di presunzioni volte a facilitare l'onere della prova da parte del danneggiato condizionate alla mancata risposta del fabbricante alla richiesta di rivelare i requisiti di funzionamento del sistema che trovano giustificazione nell'esigenza di rilanciare l'innovazione e incentivare la produzione e lo scambio di prodotti e servizi basati sull'intelligenza artificiale, mantenendo un grado di tutela soddisfacente per il danneggiato.

Lo schema concettuale concepito nella bozza non è distante, riguardo alla presunzione di nesso di causalità, da quello dettato nella nuova direttiva prodotti (UE 2024/2853) che adegua le norme sulla responsabilità per danno da prodotto difettoso a prodotti come software, sistemi di AI o servizi digitali correlati a prodotti, pur prevedendo la proposta sulla responsabilità per danno da intelligenza artificiale una diversa articolazione del regime, basata su un sistema di presunzioni che alleggeriscono l'onere probatorio del

---

[37] Sul punto si rinvia ad un successivo approfondimento. *Ex aliis* e oltre agli autori citati in nota 1, v. il contributo al dibattito di C. Scognamiglio, *Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?*, in *Resp. civ. prev.,* 2023, 1073, spec. 1088, che, in attesa della direttiva, predilige il criterio enunciato nell'art. 2050 c.c.; per uno sguardo critico sull'applicabilità delle norme interne vigenti v. Bertolini, *Intelligenza artificiale e responsabilità civile*, *Problema, sistema, funzioni*. Bologna, 2025; a favore dell'idea secondo cui i sistemi di intelligenza artificiale dovrebbero essere considerati quali centri autonomi di imputazione della responsabilità Arnaudo, Pardolesi, Ecce robot. *Sulla responsabilità dei sistemi adulti di intelligenza artificiale*, in *Danno e resp*., 2023, 409 ss. Recentemente per una ricostruzione delle questioni: Cerea, *Responsabilità civile e "sistemi intelligenti"*, Torino, 2024.

danneggiato per ragioni riconducibili alla complessità dei sistemi di intelligenza artificiale e per ovviare alla conseguente difficoltà di dimostrare che un determinato input abbia provocato un risultato (output) fonte di danno, pur restando l'individuazione dei criteri di accertamento della colpa rimessa alla legislazione dei singoli Paesi dell'UE.

L'identificazione di una disciplina in tema di responsabilità adeguata alle nuove tecnologie presenta criticità soprattutto sul piano dell'inquadramento sistematico e del grado di adattamento delle norme vigenti alle peculiarità delle situazioni generate dall'utilizzo sempre più esteso di sistemi di AI e di strumentazioni robotiche; gli interrogativi vertono sull'individuazione di profili di responsabilità oggettiva o di negligence, sul coinvolgimento di soggetti a vario titolo partecipi del processo automatizzato (produttore, proprietario, utilizzatore), sulla imprevedibilità di eventi pregiudizievoli. Anche altri profili, come quelli riguardanti la circolazione dei dati e, in particolare, la natura giuridica del dato personale, i requisiti dei contratti stipulati tra le parti per l'uso di prodotti connessi alla rete e servizi correlati, la validità delle clausole inserite, soggette ad una regolamentazione specifica, destano interesse dal punto di vista classificatorio, suscitando spunti per una lettura integrata dei testi normativi e una razionalizzazione dei relativi contenuti alla luce delle nuove istanze economiche, sociali, culturali.

Pur nella difficoltà dell'individuazione di una disciplina compatibile con i nuovi paradigmi dettati dall'evoluzione tecnologica, emerge dal panorama normativo delineato a livello europeo la necessità urgente di cogliere le sfide lanciate nell'ambito del mercato digitale che, auspicabilmente con il contributo scientifico del giurista, dovranno necessariamente tradursi in scelte di politica legislativa orientate a permettere la condivisione dei benefici derivanti dal progresso scientifico e a garantire una sinergia tra innovazione e protezione dei diritti fondamentali da cui derivino vantaggi per l'intera collettività nel rispetto dei valori dell'ordinamento.

Abstract

L'articolo affronta il tema della circolazione dei dati e dei profili giuridici dell'uso dell'intelligenza artificiale nel mercato europeo attraverso la ricostruzione della normativa contenuta nei recenti regolamenti emanati in campo digitale, con attenzione alle relazioni tra le diverse discipline declinate. L'A. rileva come la stratificazione legislativa attuata nell'ambito della *Digital Economy* richieda una valutazione della portata applicativa delle norme introdotte alla luce delle categorie generali civilistiche.

The paper examines the issue of data circulation and the legal profiles of the use of artificial intelligence in the European market through the reconstruction of the rules contained in the recent regulations issued in the digital field, with a focus on the relations between the different disciplines declined. The author highlights how the legislative stratification implemented in the Digital Economy requires an assessment of the applicative scope of the rules adopted in the light of the general civil law categories.