UNIVERSITÀ DEGLI STUDI DI MACERATA

CORSO DI DOTTORATO DI RICERCA IN
DIRITTO E INNOVAZIONE

CICLO 38°

TITOLO DELLA TESI
GOVERNO DEI DATI E POLITICHE *DATA-DRIVEN* PER IL TERRITORIO E LE IMPRESE.

SUPERVISORE DI TESI
Chiar.mo Prof. Simone Calzolaio

DOTTORANDO
Dott.ssa Camilla Lobascio

COORDINATORE
Chiar.mo Prof. Massimo Meccarelli

ANNO 2026

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani Piano Nazionale di Ripresa e Resilienza | vitality ecosistema di innovazione, digitalizzazione e sostenibilità per l'economia diffusa nell'Italia centrale

"This work has been funded by the European Union - NextGenerationEU under the Italian Ministry of University and Research (MUR)National Innovation Ecosystem grant ECS00000041 – VITALITY, MUR D.D. n. 3277/2021, CUP n° D83C22000710005"

I punti di vista e le opinioni espresse sono tuttavia solo quelli degli autori e non riflettono necessariamente quelli dell'Unione europea o della Commissione europea. Né l'Unione europea né la Commissione europea possono essere ritenute responsabili per essi".

La presente tesi di dottorato è stata realizzata nell'ambito del Progetto VITALITY – Ecosistema dell'Innovazione, Digitalizzazione e Sostenibilità per l'Economia Diffusa nell'Italia Centrale (ECS00000041), finanziato dal Ministero dell'Università e della Ricerca nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 4 "Istruzione e Ricerca", Componente 2 "Dalla ricerca all'impresa", Investimento 1.5 "Creazione e rafforzamento di ecosistemi dell'innovazione per la sostenibilità"*,con fondi dell'Unione Europea – NextGenerationEU.*

INDICE

INDICE DELLE TABELLE 4

INDICE DELLE FIGURE 5

TAVOLA DELLE SIGLE 6

PREMESSA 7

INTRODUZIONE 8

CAPITOLO I EVOLUZIONE DEL DIRITTO EUROPEO DEI DATI E DELLA DATA GOVERNANCE 16

1.1 Introduzione al diritto europeo dei dati e della data governance 16

1.2 Lo sviluppo del diritto alla *privacy* da un punto di vista dottrinale 24

1.2.1 La privacy secondo una prospettiva storico-filosofica 24

1.2.2 La privacy negli ordinamenti giuridici 29

1.3 Il diritto alla protezione dei dati personali nell'ordinamento dell'Unione Europea 38

1.3.1 La normativa europea in materia di privacy antecedente al 'nuovo' "Pacchetto Protezione Dati" 38

1.3.2 Il Regolamento UE 2016/679 (General Data Protection Regulation) 46

1.4 Il Data Governance Act 54

1.5 Il Data Act 64

1.6 Intelligenza artificiale tra trattamento di dati personali e governance nell'AI Act 74

1.6.1 Intelligenza artificiale e dati personali 74

1.6.2 La governance dell'intelligenza artificiale 83

CAPITOLO II MERCATO DEI DATI PERSONALI TRA COMMERCIALIZZAZIONE E PROTEZIONE.....92

2.1 Big Data e mercato digitale 92

2.2 La mercificazione dei dati secondo la lettura "patrimonialistica".....97

2.3 Il consenso e le sue fragilità nel mercato dei dati.....104

2.4 Proprietà, controllo e uso dei dati: modelli normativi a confronto...112

2.5 Il diritto alla portabilità dei dati tra *datification* e *data protection by design* 122

2.6 "Interoperable Europe Act" e il Mercato Unico Digitale Europeo...128

CAPITOLO III SICUREZZA E GOVERNANCE DEI DATI.....142

3.1 Sicurezza dei dati e cibersicurezza 142

3.2 Data Governance, definizione e funzioni.....156

3.3 Valutazione del rischio.....168

3.3.1 Valutazione del rischio privacy.....168

3.3.2 Gli strumenti di valutazione del rischio.....176

3.4 Valutazione di impatto (Data Protection Impact Assessment).....189

3.5 Data Breach e Severity Calculator.....204

3.6 La famiglia degli Standard ISO/IEC 27000 220

CAPITOLO IV EUROPEAN HEALTH DATA SPACE (EHDS).....227

4.1 Lo Spazio Europeo dei Dati Sanitari 227

4.2 La protezione dei dati sanitari 236

4.3 Il riutilizzo dei dati sanitari per uso primario 245

4.4 Il riutilizzo dei dati sanitari per uso secondario.....254

CONCLUSIONI 271

BIBLIOGRAFIA.....279

SITOGRAFIA 312

RIFERIMENTI NORMATIVI.....316

GIURISPRUDENZA.....321

ALLEGATI 323

INDICE DELLE TABELLE

Tabella 1 Individuazione dell'operazione di trattamento secondo il modello ENISA 178
Tabella 2 Classificazione dell'impatto secondo il modello ENISA 180
Tabella 3 Impatto derivante dalla perdita di riservatezza, integrità e disponibilità 181
Tabella 4 Valutazione delle minacce secondo il modello ENISA. 183
Tabella 5 Livello complessivo di rischio secondo il modello ENISA. 187
Tabella 6 Tipologie di dati relativi alla salute 240
Tabella 7 Fonti emergenti di dati sanitari e le loro applicazioni.....258

INDICE DELLE FIGURE

Figura 1 Principi fondamentali relativi alla DPIA. 202
Figura 2 Fasi del processo iterativo generico per lo svolgimento di una DPIA.....202

TAVOLA DELLE SIGLE

AGCM – Autorità Garante della Concorrenza e del Mercato

AI / IA – Artificial Intelligence/Intelligenza Artificiale

DA – Data Act

DGA – Data Governance Act

DMA – Digital Markets Act

DSA – Digital Services Act

DPD – Data Protection Directive (Direttiva sulla protezione dei dati)

DPA – Data Protection Authority (Autorità per la protezione dei dati)

DPO – Data Protection Officer

DPIA – Data Protection Impact Assessment

EDPB – European Data Protection Board

EHR – Electronic Health Record

EHDS – European Health Data Space

FSE – Fascicolo Sanitario Elettronico

GDPR – General Data Protection Regulation

GEPD – Garante Europeo per la Protezione dei Dati

NIS – Network and Information Security

SSN – Servizio Sanitario Nazionale

PREMESSA

Genesi della ricerca

La presente tesi di dottorato si inserisce all'interno del progetto VITALITY (Ecosistema Innovazione, Digitalizzazione e Sostenibilità per l'economia diffusa nel Centro Italia), finanziato dal PNRR, che coinvolge università, enti di ricerca e imprese delle regioni Abruzzo, Marche e Umbria. Il progetto mira a creare ecosistemi di innovazione volti a rafforzare la competitività dei sistemi produttivi regionali, promuovendo al contempo la sostenibilità e la qualità della vita nelle aree urbane e rurali.

La ricerca si concentra sul Work Package 3 del progetto, dedicato alle filiere industriali con alto potenziale di crescita e innovazione sociale, con l'obiettivo di promuovere reti di imprese e centri di ricerca che sviluppino nuovi modelli, servizi e tecnologie orientati all'inclusione sociale. In particolare, lo Spoke SAFINA – *Smart solutions and educational programs for anti-fragility and inclusivity*, coordinato dall'Università di Macerata, si propone di supportare la vita indipendente, l'invecchiamento attivo e lo sviluppo di filiere industriali e culturali capaci di operare in contesti inclusivi e resilienti.

All'interno di questa ricerca, la gestione sicura e responsabile dei dati richiede un equilibrio delicato tra gli usi innovativi derivati dagli avanzamenti tecnologici e la protezione dei diritti fondamentali degli individui, con particolare riguardo ai dati sanitari, altamente sensibili.

INTRODUZIONE

Negli ultimi anni, l'evoluzione tecnologica ha profondamente trasformato il modo in cui i dati vengono raccolti, trattati e utilizzati, ponendo nuove sfide al quadro normativo europeo.

La trasformazione digitale, ormai comunemente sintetizzata con il termine 'digitalizzazione', rappresenta il passaggio di tutti i fenomeni ad un formato numerico, modificando in maniera radicale diversi aspetti della nostra vita. Questo concetto viene spesso declinato con l'aggiunta del prefisso 'e', che indica la trasposizione digitale di attività e settori, come il commercio (e-commerce), la posta elettronica (e-mail), la società (e-society), il governo (e-government), l'economia (e-economy), la sanità (e-health) e l'istruzione (e-learning)[1]. Si parla di interconnessione digitale su larga scala poiché il 65% della popolazione mondiale ha accesso a internet[2], fenomeno che comporta la generazione di una massa di dati che costituiscono una merce ed alimentano la *data driven economy*.

Per regolamentare il crescente mercato digitale, l'Unione Europea ha intrapreso, a partire dal 2010, una serie di interventi normativi su vasta scala. Attraverso piani, direttive, raccomandazioni e regolamenti si è andata costruendo una complessa struttura di regole il cui obiettivo principale è quello di garantire che, nonostante la moltiplicazione degli interventi in differenti ambiti, tutti i regolamenti confluiscano verso un quadro giuridico armonizzato e coerente, capace di affrontare le sfide poste dalla digitalizzazione in un contesto in continua trasformazione.

[1] G. ALPA, *Il mercato unico digitale*, in *Contratto e impresa Europa*, 2021, 1, 1-3.
[2] A. MORACE PINELLI, *Introduzione*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 1-22.

Recentemente, si è assistito a una significativa fase di evoluzione della trasformazione digitale in Europa, caratterizzata principalmente da due sviluppi di particolare rilievo.

In primo luogo, come accennato, si è verificato un marcato aumento della normativa sovranazionale nel settore del digitale, infatti, attraverso il quadro del Mercato Unico Digitale, la Commissione Europea, il Parlamento europeo e il Consiglio hanno collaborato per introdurre nuove regolamentazioni in settori già disciplinati dall'Unione europea o per regolare completamente nuovi fenomeni. Questa evoluzione ha visto l'adozione e la proposta di regolamenti e direttive in settori chiave quali la protezione dei dati personali e non, la proprietà intellettuale (compresi brevetti, marchi e diritti d'autore), il commercio elettronico, gli intermediari online (incluse le piattaforme digitali), i servizi media audiovisivi, la tutela dei consumatori, la lotta alla criminalità digitale, la sicurezza delle reti e dei sistemi informativi, nonché l'introduzione di normative per i sistemi di intelligenza artificiale (IA). La seconda caratteristica saliente della recente fase della trasformazione digitale europea è rappresentata dall'intreccio sempre più stretto e frequente tra discipline settoriali ed elementi costituzionali fondamentali dell'Unione. Tale transizione non si limita più a essere una componente esclusiva del mercato interno né può essere considerata solamente come una sua specifica evoluzione. Si tratta piuttosto di un cambiamento più ampio che coinvolge anche l'essenza stessa dell'Unione europea: la portata potenzialmente trasformativa di una tale metamorfosi ha giustificato il progressivo sviluppo di ciò che nella dottrina è definito come "costituzionalismo digitale europeo[3]".

Come sottolineato da T. E. Frosini, il diritto è ormai da tempo entrato a far parte della società tecnologica, portando con sé le questioni e le

[3] C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in *Law and Legal Institutions*, 2024, 11, 1-34.

problematiche derivanti dall'applicazione delle tecniche giuridiche, sia sostanziali che processuali, nel vasto mondo della tecnologia, con particolare riferimento alla rete Internet. Pertanto, si potrebbe riformulare l'antico brocardo latino in "*ubi societas technologica, ibi ius*". In seguito all'avvento della tecnologia, si assiste a un nuovo modo di concepire il diritto e, di conseguenza, anche ad una metamorfosi della figura del giurista, che da umanista si trasforma in giurista tecnologico. Il ruolo di quest'ultimo è interpretare le trasformazioni che stanno avvenendo nella società a seguito dello sviluppo tecnologico e dell'impatto che questo ha sul diritto e sui diritti fondamentali[4].

L'unione tra i principi della sovranità digitale e quelli del costituzionalismo digitale costituisce un elemento chiave delle attuali politiche digitali dell'Unione Europea. Il progetto europeo si pone dunque l'obiettivo di creare un terzo approccio alla governance di Internet, che si differenzi sia dal modello di autoregolamentazione privata degli Stati Uniti, sia dal modello centralizzato governativo sostenuto dai regimi autoritari. In altre parole, si può affermare che l'UE stia lavorando, ed ha lavorato negli ultimi anni, per sviluppare un approccio distintivo che si occupi di integrare la protezione dei diritti digitali e delle libertà individuali con una efficiente regolamentazione del mercato digitale, senza però trascurare la sicurezza dei dati. Questo equilibrio tra sovranità digitale e costituzionalismo digitale prevede l'istituzione di un quadro normativo che tuteli sia gli utenti che le infrastrutture digitali, evitando un controllo centralizzato rigido od un approccio completamente *laissez-faire*[5].

---

[4] La tecnologia è da intendersi secondo la definizione di T. E. Frosini, ovvero "*il fecondo connubio di scienza e di tecnica, che si è verificato con la stimolazione della ricerca scientifica verso obiettivi pratici e con la rivalutazione della tecnica, in quanto collegata e sottomessa alla ricerca scientifica; pertanto, la tecnologia è il prodotto della scienza resa operativa.*" In: T. E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Il Diritto dell'Informazione e dell'Informatica*, 2020, 3, 465-466.

[5] M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance,* in *Rivista italiana di informatica e diritto*, 2022, 4, 47-51.

I cittadini europei contano ormai sempre di più sull'interscambio di dati e di informazioni per l'affermazione della propria identità, sia individualmente che all'interno delle proprie comunità sociali. Le implicazioni costituzionali di questa constatazione sono molteplici e segnano il passaggio dall'innovazione orientata dai dati (*data driven innovation*) alla più rigida e strutturale dipendenza sistemica dalla raccolta dei dati[6]. In questo contesto, è fondamentale osservare come diversi diritti e principi che si riferiscono alla disciplina privacy, tra cui il diritto alla portabilità dei dati e il principio di *data protection by design*, siano intimamente connessi con il fenomeno della datificazione.

L'interesse delle imprese nei confronti dei dati personali si spiega con la loro capacità di generare valore economico. I dati, infatti, una volta raccolti e sottoposti a processi di trattamento e analisi, possono essere arricchiti e riutilizzati per ottenere informazioni dotate di rilievo economico. In tal modo, essi cessano di essere meri elementi informativi e assumono la natura di veri e propri beni suscettibili di sfruttamento, entrando a far parte del patrimonio immateriale dell'impresa.

Questa trasformazione ha reso i dati personali una componente essenziale dei modelli di business basati sulla circolazione e sull'elaborazione delle informazioni, nei quali il trattamento dei dati diviene strumento di produzione e di scambio. Ne sono un esempio le piattaforme digitali che fondano la propria redditività sulla profilazione degli utenti e sulla pubblicità personalizzata, pratiche che consentono di ricavare un'utilità economica diretta a partire dal comportamento individuale. In tale prospettiva, i dati personali vengono progressivamente "patrimonializzati", fungendo da

[6] S. CALZOLAIO, *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in *Rivista italiana di informatica e diritto*, 2024, 5, 13-33; S. CALZOLAIO, *Protezione dei dati personali, aggiornamento*, in *Digesto delle discipline pubblicistiche*, UTET, 2017.

controprestazione per l'accesso ai servizi digitali e da fonte di vantaggio competitivo nei mercati online[7].

In questa prospettiva, la tutela dei dati personali si configura come elemento imprescindibile non solo per garantire la sicurezza intesa in senso oggettivo, quale protezione effettiva dei diritti e delle libertà fondamentali, ma anche per assicurare quella dimensione soggettiva di sicurezza che alimenta la fiducia dei cittadini e costituisce il tessuto connettivo delle società contemporanee. Alla luce di tale impostazione, appare dunque riduttiva la contrapposizione tradizionale tra "privacy e sicurezza": più appropriato è ritenere che la protezione dei dati personali rappresenti, essa stessa, una forma di sicurezza[8].

Si sostiene che la disponibilità e la circolazione dei dati stiano assumendo un ruolo che va oltre l'ambito economico, diventando strumenti essenziali per la protezione dei diritti fondamentali e di interessi costituzionalmente tutelati, come la salute pubblica. L'impiego combinato di tecnologie avanzate e dell'intelligenza artificiale consente oggi di migliorare la prevenzione, la diagnosi e i trattamenti sanitari personalizzati, nonché di anticipare emergenze sanitarie e climatiche. Al contempo, questo sviluppo comporta sfide e rischi sia tradizionali sia emergenti, che richiedono una gestione attenta e consapevole[9].

Per quanto concerne la struttura, la tesi si articola in quattro distinti capitoli, ciascuno dedicato a un aspetto centrale del diritto europeo dei dati e della data governance.

---

[7] V. MONTOZZI, *Le nuove sfide della regolazione dei dati: analisi di un modello a partire dall'intersezione tra protezione dei dati personali e concorrenza*, in *Rivista italiana di informatica e diritto*, 7, 2025, 501-524.

[8] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Media Laws*, 2, 2018, 82-104.

[9] M. OROFINO, *One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in *Corti Supreme e Salute*, 2025, 1, 1-19.

Il primo di essi esamina l'evoluzione dell'ordinamento giuridico europeo dei dati, a partire dall'interpretazione del concetto statunitense di privacy. L'analisi storico-dottrinale mira a evidenziare le ragioni che hanno condotto al consolidamento della protezione dei dati personali come diritto fondamentale, delineando il sistema europeo. In questo contesto, il capitolo esamina il percorso normativo dalla legislazione antecedente al più recente Pacchetto Protezione Dati fino al Regolamento UE 2016/679 (GDPR), soffermandosi inoltre su alcuni regolamenti cardine della Strategia Europea per i Dati, ovvero Data Governance Act, Data Act e AI Act, di cui vengono trattati aspetti relativi alla governance e al trattamento dei dati personali.

Il secondo capitolo si concentra sul mercato dei dati personali, esplorando le dinamiche di commercializzazione dei dati. La capacità di analisi e valorizzazione dei dati da parte dei grandi operatori digitali su scala globale ha creato nuove forme di sfruttamento economico e di profilazione algoritmica a fini commerciali, generando concentrazioni di potere. Ne derivano nuove problematiche giuridiche legate alla "commercializzazione" dei dati personali, cioè alla possibilità di attribuire al dato un valore economico, equiparabile a quello della moneta. Nel mercato digitale attuale, il dato ha acquisito un valore patrimoniale sia per gli operatori economici, sia per i consumatori/utenti, che sono spesso obbligati a fornire i propri dati per accedere a servizi solo apparentemente gratuiti[10]. Particolare attenzione è dedicata ai Big Data, alle ambiguità del consenso, ai modelli di proprietà e controllo dei dati, nonché al diritto alla portabilità nell'ottica della data protection by design. Viene inoltre analizzato il ruolo dell'Interoperable Europe Act all'interno del Mercato Unico Digitale Europeo.

Il terzo capitolo approfondisce gli aspetti legati alla sicurezza, alla protezione e alla governance dei dati, tramite un'analisi incentrata sulla

[10] V. BARELA, *Accezione aggregata del dato: shuffle degli interessi in gioco e necessità di un approccio interdisciplinare a presidio del diritto di autodeterminazione della persona*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2023, 159-187.

protezione dei singoli utenti e sull'insieme di tecnologie, processi e procedure finalizzate alla protezione di reti, dispositivi, programmi e dati da attacchi, danni o accessi non autorizzati.

Infine, il quarto capitolo è dedicato allo European Health Data Space (EHDS). Con l'entrata in vigore, a marzo 2025, del Regolamento sullo Spazio Europeo dei Dati Sanitari, viene completata un'importante tappa della Strategia europea per i dati, avviata dalla Commissione Europea nel febbraio 2020. Lo Spazio Europeo dei Dati Sanitari mira a superare le barriere che ostacolano la condivisione e l'uso efficace delle informazioni sanitarie tra Stati membri e a rafforzare i diritti dei pazienti sui loro dati sanitari elettronici. Il Regolamento prevede due principali modalità di utilizzo dei dati sanitari: l'uso primario, destinato al trattamento dei dati per i pazienti a fini di cura, assicurando un accesso tempestivo; e l'uso secondario, che consente a ricercatori e soggetti economici pubblici e privati di impiegare i dati per scopi di interesse generale, come istruzione, ricerca scientifica, sviluppo e innovazione[11].

In sintesi, l'elaborato si propone di offrire una lettura organica del diritto europeo dei dati, integrando profili storici, dottrinali, normativi e tecnologici, al fine di comprendere le sfide poste dalla digitalizzazione, dalla circolazione dei dati e dall'introduzione di nuovi strumenti di governance, inclusa l'intelligenza artificiale, nel contesto europeo.

Alla luce delle considerazioni svolte, la scelta di articolare l'elaborato in quattro capitoli risponde all'esigenza di ricostruire il diritto europeo dei dati seguendo un percorso logico e progressivo, capace di mettere in relazione l'evoluzione normativa con le trasformazioni economiche e tecnologiche in atto. Per le ragioni descritte l'analisi prende avvio dall'affermazione della protezione dei dati personali come diritto fondamentale, la quale rappresenta

[11] E. CALZOLAIO, *Il regolamento sullo Spazio dei dati sanitari nella prospettiva della cittadinanza europea*, in *Diritto dell'Informazione e dell'Informatica*, 3, 2025, 315-335.

un passaggio imprescindibile per comprendere le scelte regolatorie adottate dall'Unione Europea e il successivo sviluppo di un sistema articolato di data governance. Su queste basi si innesta l'esame del mercato dei dati personali, nel quale il dato assume un ruolo centrale non solo come oggetto di tutela, ma anche come risorsa economica, generando nuove tensioni tra protezione dei diritti, modelli di business e concentrazioni di potere. Tale scenario rende necessario un approfondimento degli strumenti di sicurezza, protezione e gestione del rischio, indispensabili per garantire un uso responsabile dei dati e l'effettività delle garanzie previste dall'ordinamento. Il percorso arriva alla sua conclusione con l'analisi dello European Health Data Space, ambito nel quale le problematiche affrontate nei capitoli precedenti trovano una concreta applicazione, mostrando in modo emblematico la complessità del bilanciamento tra circolazione dei dati, innovazione, interesse pubblico e tutela dei diritti fondamentali. Nel loro insieme, i capitoli intendono offrire una lettura organica del diritto europeo dei dati, evidenziandone la coerenza interna e le principali criticità emergenti.

CAPITOLO I
EVOLUZIONE DEL DIRITTO EUROPEO DEI DATI E DELLA DATA GOVERNANCE

Sommario: 1.1 Introduzione al diritto europeo dei dati e della data governance – 1.2 Lo sviluppo del diritto alla "privacy" da un punto di vista dottrinale – 1.2.1 La privacy secondo una prospettiva storico-filosofica – 1.2.2 La privacy negli ordinamenti giuridici – 1.3 Il diritto alla protezione dei dati personali nell'ordinamento dell'Unione Europea – 1.3.1 La normativa europea in materia di privacy antecedente al "nuovo" Pacchetto Protezione Dati – 1.3.2 Il Regolamento UE 2016/679 (General Data Protection Regulation) – 1.4 Il Data Governance Act – 1.5 Il Data Act – 1.6 Intelligenza artificiale tra trattamento di dati personali e governance nell'AI Act– 1.6.1 Intelligenza artificiale e dati personali – 1.6.2 La governance dell'intelligenza artificiale

1.1 Introduzione al diritto europeo dei dati e della data governance

La materia oggetto del presente studio è quella relativa alla *data governance* (o governo dei dati). Questo ambito è stato una priorità nell'agenda normativa dell'Unione Europea per più di un decennio, a partire dal 25 gennaio 2012, anno in cui la Commissione ha adottato un pacchetto di misure per la riforma delle norme dell'Unione in materia di protezione dei dati, che comprendeva sia una proposta di regolamento contenente il quadro normativo generale in materia di protezione dei dati, sia una proposta di direttiva sulla protezione dei dati nel settore delle attività di contrasto[12].

[12]Garante europeo della protezione dei dati (GEPD), *Sintesi del parere del GEPD del 7 marzo 2012 sul pacchetto di riforma della protezione dei dati*, http://www.edps.europa.eu, consultato da ultimo il 14.10.2025.

La Commissione, a partire dal 2016, ha intrapreso diverse iniziative, tra cui si ricorda l'istituzione da parte dell'Unione Europea di uno dei più solidi quadri per garantire ai suoi cittadini la fiducia digitale, il Regolamento generale sulla protezione dei dati personali (GDPR)[13]. Sono da segnalare altre iniziative che hanno dato una spinta allo sviluppo dell'economia dei dati, ovvero il Regolamento sulla libera circolazione dei dati non personali[14], il Regolamento sulla cibersicurezza[15] e la Direttiva relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico[16].

Il modello europeo di protezione dei dati ha perseguito, negli anni, una molteplicità di obiettivi la cui volontà è stata quella di diventare un riferimento per una società che, grazie ai dati, dispone degli strumenti necessari per adottare decisioni migliori, sia a livello imprenditoriale che pubblico. Per rendere concreta tale ambizione, l'UE può ora fare affidamento, in primo luogo, su un quadro giuridico solido, in termini di protezione dei dati, dei diritti fondamentali, della sicurezza e cibersicurezza, ma anche sul suo mercato interno, caratterizzato da imprese competitive (di ogni dimensione) e da una base industriale piuttosto diversificata[17].

Nell'ampio contesto normativo europeo si è aggiunta, più recentemente, anche la Strategia Europea per i Dati della Commissione europea, presentata il 19 febbraio 2020, il cui scopo è quello di delineare degli

[13] 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 e alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati).
[14] Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018 relativo alla libera circolazione dei dati non personali nel mercato interno.
[15] Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo a un quadro europeo per la cibersicurezza (Cybersecurity Act).
[16] Direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio del 20 giugno 2019 relativa all'open data e alla riutilizzazione dell'informazione del settore pubblico (Direttiva sull'open data)
[17] Commissione europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni del 19 febbraio 2020, *Una strategia europea per i dati*, COM(2020) 66 final.

obiettivi e delle linee di intervento per realizzare misure politiche e investimenti a sostegno dell'economia dei dati fino al 2025[18].

Il significativo impatto delle discipline europee, in grado di sviluppare una influenza normativa a livello globale, dovuto al peso del mercato europeo e in coerenza con gli interessi dell'Unione Europea, va a costituire il fenomeno denominato come "*Brussels effect*"[19]. Questo avviene perché, sebbene l'Unione Europea disciplini formalmente soltanto il proprio mercato interno, le imprese multinazionali hanno spesso interesse a uniformare la produzione a livello globale e ad attenersi a un unico insieme di regole. In questo modo, la normativa europea tende a proiettarsi oltre i confini dell'Unione, trasformandosi di fatto in uno standard globale[20]. Le pronunce e gli interventi indicati si collegano al tentativo della disciplina europea di voler "esportare" un proprio modello regolativo al di fuori del territorio degli stati membri dell'Unione, sotto forma di buone regole, seguendo il modello del GDPR, la cui influenza è esercitata anche su altri ordinamenti.

Attualmente è un numero piuttosto esiguo di imprese tecnologiche non-europee (*Big Tech*) a detenere il pieno controllo sulla maggior parte dei dati disponibili ma, tramite l'ultimo regolamento europeo sui dati (Data Act), entrato in vigore a gennaio 2024, la Commissione mira a rendere disponibile per l'uso un maggior numero di dati e a stabilire norme su chi può utilizzarli e accedervi e per quali scopi in tutti i settori economici dell'UE. È chiara, dunque, l'intenzione di perseguire un'indipendenza digitale europea nei confronti di Stati Uniti e Cina, andando a riaffermare una sovranità digitale europea. L'attenzione dell'Unione Europea sui temi legati all'utilizzo dei dati, sia attraverso regolazioni *ex ante* che controlli *ex post*, potrebbe favorire

[18] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi Parlamentari e di Politica Costituzionale*, 2021, 209, 31-52.
[19] S. CALZOLAIO, *Protezione dei dati personali*, in *Digesto delle discipline pubblicistiche*, Milano, UTET Giuridica, 2017.
[20] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford-New York, Oxford University Press, 2020.

l'emergere di un terzo modello di disciplina per le economie data-driven, in grado di trovare un equilibrio tra il sistema americano e quello cinese.

Nel contesto americano, la tendenza si concentra sulla promozione dell'efficienza del mercato, andando a favorire gli interessi privati e provocando una significativa concentrazione di potere. Al contrario, il modello cinese[21] privilegia principalmente l'utilizzo pubblico dei dati, sollevando importanti questioni riguardanti il rispetto dei diritti fondamentali e il fenomeno della sorveglianza di massa.

In questo scenario, il modello europeo potrebbe essere sintetizzato nella mediazione tra le esigenze economiche pro-concorrenziali e le istanze sociali legate al rispetto dei diritti fondamentali. L'obiettivo sarebbe proprio quello di sviluppare un modello di riferimento per la raccolta e l'utilizzo dei dati che metta al centro l'interesse dell'individuo, in linea con i valori, i diritti fondamentali e le normative europee. Infatti, la Commissione europea stessa ha espresso la volontà politica di far diventare l'Unione un modello di riferimento globale per l'economia digitale[22]. Quanto descritto sta però avvenendo con un pesante ritardo, in un mercato in cui una disciplina relativa alla governance dei dati sembra indispensabile per cercare di recuperare il terreno perso nel posizionamento del mercato dei dati e, di conseguenza, dell'*Information Technology*.

---

[21] Nel 2021, il legislatore cinese ha rivolto una rinnovata attenzione alla regolamentazione dei dati con l'introduzione della *Data Security Law* e della *Personal Information Protection Law*. Queste normative, insieme alla *Cybersecurity Law* del 2017, costituiscono il quadro giuridico per la gestione, l'uso e la protezione dei dati nella Repubblica Popolare Cinese, in linea con gli obiettivi del piano quinquennale per lo sviluppo dell'economia digitale. I dati, considerati una risorsa strategica per il Paese, sono definiti come "informazioni registrate in formato elettronico o altri formati" (art. 3, co. 1, DSL) e vengono classificati in "dati fondamentali dello Stato", "dati importanti" e "dati generali" (art. 2, DSL), ognuno soggetto a regimi giuridici diversi. Per quanto riguarda i dati personali, una categoria trasversale, è stata introdotta una disciplina specifica attraverso la Personal Information Protection Law, influenzata in alcuni aspetti dal GDPR europeo. M. TIMOTEO, *Alla ricerca di un diritto di proprietà dei dati. La via cinese*, in *Rivista Trimestrale di Diritto e Procedura Civile*, 2023, 4, 1157-1174.

[22] A. SOLA, *Primi cenni di regolazione europea nell'economia dei dati*, in *Media Laws*, 2021, 3, 188-209.

In tale contesto è chiaro come i dati si siano affermati come "bene economico" (*economic good*)[23], capaci di creare ricchezza per la società, prestare capacità di controllo ai cittadini e diffondere fiducia alle imprese. Si legge, nella Strategia Europea per i Dati, che: "*i dati ridefiniranno il nostro modo di produrre, consumare e vivere, generando benefici percepibili in ogni singolo aspetto della nostra vita: da un consumo energetico più consapevole alla tracciabilità dei prodotti, dei materiali e degli alimenti, da una vita più sana a una migliore assistenza sanitaria.*"

I dati sono fondamentali per sostenere lo sviluppo economico, poiché consentono di offrire più servizi ai cittadini, migliorano la produttività e ottimizzano l'uso delle risorse in diversi settori dell'economia. Essi contribuiscono nel favorire anche la crescita di nuove start-up e delle piccole e medie imprese, nella creazione e distribuzione di nuovi prodotti e servizi.

È importante segnalare la particolare attenzione rivolta dall'Unione al mercato dei dati personali e alle dinamiche concorrenziali nella fornitura dei servizi, come è stato già avvertito nelle scelte che hanno animato il GDPR. In particolar modo si evidenzia il diritto alla *data portability*, o alla portabilità dei dati, descritto dall'art. 20 del GDPR come il diritto dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento ed il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti[24].

---

[23] N. PURTOVA, G. VAN MAANEN, *Data as an economic good, data as a commons, and data governance*, in *Law, Innovation and Technology*, 2023, 16(1), 1-42.

[24] Quanto descritto è valido nei casi in cui il trattamento si basi sul consenso o su un contratto ai sensi dell'articolo 6, o il trattamento sia effettuato con mezzi automatizzati. Ciò viene reso possibile anche nel caso in cui il secondo titolare indicato dall'interessato sia un competitor del primo nella fornitura di un determinato servizio. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, 199-256.

Giustappunto, i modelli di business delle piattaforme digitali maggiormente diffusi si fondano prevalentemente su operazioni che implicano uno scambio di dati, le quali si configurano come prestazioni non di natura monetaria, bensì basate sulla cessione di dati personali forniti o generati dall'utente, quale corrispettivo per l'accesso e l'utilizzo del servizio offerto. Questo fenomeno si estende a tutta la nostra società, sempre più caratterizzata dall'offerta di beni e servizi digitali, in cui le capacità di governo dei dati quotidianamente generati assumono un ruolo essenziale nel determinare non solo i rapporti fra privati, ma anche quelli tra imprese e istituzioni. Nel quadro delineato, in ogni settore, si assiste dunque ad una evoluzione pressoché continua (*rectius transizione*), di tutte le attività verso una transizione digitale, che ha come effetto diretto la datificazione correlata ai beni e servizi offerti. Se i nuovi orizzonti che le applicazioni tecnologiche consentono di raggiungere in termini di progresso scientifico sono necessari e significativi per le comunità, si rende però necessario considerare tutte le ricadute di matrice economica, sociale e culturale che una evoluzione talmente repentina comporta[25].

In merito, il "Data Act" e il recente regolamento "Data Governance Act" si configurano come disposizioni normative intercomunicanti, miranti alla configurazione di un inedito modello "europeo" di governance dei dati. Tale progetto è volto, da un canto, a temperare l'accresciuto arbitrio accentrato presso soggetti situati al di fuori dell'Unione, sia essi enti pubblici che entità private, e, dall'altro, a custodire l'integrità sovrana degli Stati membri mediante il contenimento della mole di dati che, varcando i confini europei, potrebbero divenire appannaggio di autorità o industrie extracomunitarie[26]. Si parla ormai di regolamentazione multilivello, poiché

[25] D. AMRAM, *Governo dei dati, Open AI e salute: profili introduttivi*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2023, 2, 293-299.
[26] S. TORREGIANI, *Il Data Act: una versione europea del Data Nationalism?*, in *Rivista italiana di informatica e diritto*, 2024, 5(2), 131-146.

gli interventi del legislatore europeo (pressoché "alluvionali") devono essere in accordo e in coordinazione con il resto dei pilastri della Strategia Europea per i Dati. Per esempio, sarà, in un certo senso, il Data Act a rispondere ad alcune osservazioni generate dal Data Governance Act (si pensi al contratto di condivisione dei dati) e una normativa rimanderà all'altra in questo senso[27].

In breve, l'Unione Europea ha adottato un approccio strategico alla regolazione, caratterizzato da una chiara visione sistemica. Il quadro normativo introdotto finora, che si compone di GDPR (pilastro e modello per i regolamenti a venire), Artificial Intelligence Act (AI Act), Digital Services Act (DSA), Digital Markets Act (DMA), fino ai più recenti Data Act (DA), Data Governance Act (DGA), Open Data Directive, insieme al Regolamento sullo spazio europeo dei dati sanitari "European Health Data Space" (EHDS) e alla Direttiva NIS2, ha avviato un vero e proprio processo costituente. Elemento imprescindibile di questo sistema è la garanzia di un riutilizzo sicuro dei dati personali e delle informazioni commerciali riservate per scopi di ricerca, innovazione e analisi statistica. Tale obiettivo può essere conseguito mediante l'applicazione di tecniche di tutela avanzata – come l'anonimizzazione, la pseudonimizzazione, la privacy differenziale, la generalizzazione o la randomizzazione – che consentono l'elaborazione dei dati senza compromettere la riservatezza degli individui[28]. In questo modo, imprese e cittadini possono avere la certezza che l'utilizzo di categorie sensibili di dati avverrà nel pieno rispetto dei loro diritti e interessi legittimi[29].

Questo ricco sistema stabilisce un insieme di diritti per gli utenti della rete, limitando il potere delle piattaforme dominanti, creando nuove autorità

[27] D. POLETTI, *Il quadro normativo del Data Governance Act: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 65-82.

[28] Come verrà discusso, anche queste tecniche non sono da considerarsi esenti da rischi per i diritti degli interessati.

[29] M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Rivista italiana di informatica e diritto*, 2021, 3(2), 7-23.

e conferendo nuovi poteri sia alle istituzioni europee che nazionali, imponendo loro obblighi e fissando limiti alla loro azione[30]. La scelta di puntare sulla regolamentazione sembra derivare da una certa consapevolezza, all'interno dell'Unione, del ritardo accumulato rispetto ai suoi concorrenti globali in termini di ricerca e sviluppo di nuove tecnologie[31]. In tale prospettiva, assume rilievo la definizione di una cornice di governance a livello europeo che disciplini, tra l'altro, il riutilizzo di dati detenuti dal settore

[30] Prima di arrivare alla definizione di alcuni dei regolamenti descritti, è interessante segnalare come il pensiero relativo alla regolamentazione della rete si sia evoluto. Nel 1996, J. P. Barlow, nella sua "*A Declaration of the Independence of Cyberspace*", sosteneva che il cyberspazio fosse un territorio privo di sovranità, dove la governance non solo non fosse auspicabile, ma neppure realizzabile. Secondo Barlow, la partecipazione del legislatore nel cyberspazio era fuori discussione, in particolare per quanto riguardava tematiche come la libertà di espressione, e non veniva nemmeno riconosciuto il potere esecutivo dello Stato. Quanto affermato è in linea con l'idea preponderante nel secolo scorso per cui la tecnologia sembrava affermarsi come un fenomeno indipendente dalla normativa, ma, con il tempo è diventato evidente quanto fosse profonda la connessione tra i due ambiti, portando i giuristi ad interrogarsi sulla necessità di una governance specifica per regolamentare il cyberspazio. Questo perché concetti come la proprietà intellettuale e le implicazioni legali delle azioni svolte online, inclusi reati come hacking, phishing, violazione di copyright, cyberbullismo mal si conciliavano con la visione di Barlow. Questi crimini evidenziavano la necessità di una regolamentazione specifica per garantire la sicurezza e l'affidabilità delle tecnologie. Inoltre, l'espansione degli e-commerce, la contrattazione elettronica e l'erogazione di servizi online rendevano inevitabile l'intervento legislativo per favorire l'adozione sicura di queste nuove tecnologie. (J. P. BARLOW, *A Declaration of the Independence of Cyberspace*, 8 febbraio 1996, pubblicato online da Electronic Frontier Foundation, consultato su https://www.eff.org/cyberspace-independence, consultato da ultimo il 14.10.2025.) Una visione alternativa della governance di Internet rispetto a quella di Barlow è quella proposta da L. Lessig. Con la formula "*Code is Law*", tratto dal suo libro "*Code and Other Laws of Cyberspace"* (1999), Lessig riprende il termine della "*Lex informatica*" di J. Reidenberg (J. R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, 1997, 76(3), 553-593) e sottolinea il ruolo crescente del codice come norma regolatrice. Secondo Lessig, il codice diventa fondamentale nel disciplinare le interazioni e i comportamenti degli utenti online, indicando un processo spontaneo e inevitabile che si sviluppa nel cyberspazio. In questo contesto, Lessig afferma che la libertà nel cyberspazio non deriverebbe dall'assenza dello Stato, ma dalla sua capacità di esercitare un controllo moderato, favorendo un ambiente in cui la libertà possa prosperare. In tal modo, si passa dalla visione radicale di Barlow, che rifiutava l'intervento del legislatore, a un approccio più equilibrato che riconosce il ruolo della regolamentazione, pur mantenendo il codice come punto di riferimento principale. (I. MARCOLONGO et al., *Internet governance: una questione di digital trust*, in *Rivista italiana di informatica e diritto*, 4(1), 2022, 241-250).

[31] S. DEL GATTO, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation. Il caso del riconoscimento facciale*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2023, 1, 37-64.

pubblico, l'attività dei fornitori di servizi di intermediazione tra utenti e imprese (come i marketplace), nonché l'impiego a fini altruistici delle informazioni messe a disposizione da soggetti privati o istituzionali.

1.2 Lo sviluppo del diritto alla *privacy* da un punto di vista dottrinale

1.2.1 La privacy secondo una prospettiva storico-filosofica

La disciplina della privacy riveste un ruolo fondamentale, in quanto definisce il quadro giuridico per il trattamento e la protezione dei dati personali nell'Unione Europea. Analizzarne l'evoluzione consente di comprendere a fondo il funzionamento e le caratteristiche del sistema attuale, offrendo una chiave di lettura per interpretare le sue norme e i suoi principi. La riflessione sulla tutela della c.d. *privacy*, o più propriamente della riservatezza, solleva interrogativi giuridici di non poco momento. La dottrina sul punto è ampia e articolata: si discute, talora in modo sovrapponibile ma non sempre univoco, di *privacy*, *privatezza*, *vita privata* e *riservatezza*, termini che evocano sfumature concettuali distinte e che talvolta generano incertezza definitoria[32].

In particolare, il concetto di *privacy*, inteso come diritto tipico dell'"età d'oro della borghesia", entra nel panorama giuridico italiano in maniera esplicita solo con l'art. 8 della legge 20 maggio 1970, n. 300 (*Statuto dei lavoratori*[33]), che sancisce il divieto di indagare sulle opinioni politiche,

[32] In italiano il termine *privacy* viene solitamente reso con parole come "riservatezza", "privatezza" o "sfera privata". Si tratta di un concetto che ricorre sia nel linguaggio quotidiano, sia nel dibattito filosofico, politico e giuridico. Tuttavia, non esiste una definizione univoca o definitiva che ne esaurisca il significato. Al contrario, il senso attribuito alla parola ha conosciuto trasformazioni continue: pur mantenendo inalterata la forma linguistica, la *privacy* ha assunto nel tempo sfumature diverse, adattandosi ai mutamenti sociali, culturali e tecnologici che ne ridefiniscono costantemente i confini.

[33] L. 20 maggio 1970, n. 300 "Norme sulla tutela e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento".

religiose o sindacali dei lavoratori[34]. Si tratta di un primo riconoscimento normativo della sfera privata come ambito intangibile rispetto all'invadenza datoriale[35].

Nella storia della cosiddetta "civiltà occidentale" – espressione che richiede le dovute cautele – la privacy non costituisce una nozione originaria né una categoria fondativa tale da poter essere ricostruita a partire da un principio primo, *ex arches*[36].

Per Aristotele, la famiglia (nel suo lessico l'*oikos*, o talvolta l'*oikia*) rappresentava l'unità sociale fondamentale della *polis*. Il nucleo familiare della Grecia Antica descritto da Aristotele era caratterizzato dall'associazione con la vita domestica, distinta dalla vita politica e pubblica. Tra *oikos* e polis vi era una costante linea di tensione e spesso entravano in conflitto fra loro. Da una parte, l'*oikos*, essendo la singola unità familiare che componeva la polis, poteva influenzarne le decisioni pubbliche; dall'altra, la *polis*, qualora lo ritenesse necessario, poteva emanare leggi che interferivano significativamente con la vita nell'*oikos* (come, ad esempio, le leggi relative alla cittadinanza o al matrimonio[37]). Le relazioni tra *oikia* e *polis* possono essere viste come prime rappresentazioni storiche dell'interazione tra spazi privati e pubblici[38]. Lo spazio pubblico può essere inteso come la dimensione

[34] Con l'evidente paradosso per cui ciò che era nato come un diritto tipico della borghesia è entrato nell'ordinamento giuridico positivo italiano attraverso una legge volta alla tutela dei lavoratori e di uno dei diritti sociali per eccellenza: il lavoro. E. BRUGIOTTI, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Riv. on-line Dir. Fondam.*, 2013, 2, 9.
[35] S. ORLANDO, *La tutela penale della privacy nel cyberspazio*, in *Diritto penale contemporaneo – Rivista Trimestrale*, 2019, 2, 177-194.
[36] V. COLOMBA, G. ZANETTI, *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in *Teoria e Critica della regolazione sociale*, 2017, 1, 27-39.
[37] J. ROY, *Polis and Oikos in Classical Athens*, in *Greece and Rome*, 1999, 46(1), 1-18.
[38] Il rapporto tra lo spazio del governo politico, riservato esclusivamente agli uomini, e la sfera domestica e familiare, nella quale la donna viene relegata, non consente ancora di parlare di una rivendicazione giuridica di un diritto alla privacy come espressione della dignità personale e come perno di delimitazione e legittimazione delle istituzioni pubbliche. Solo con l'affermarsi della concezione moderna dell'uomo come soggetto capace di volere e di agire autonomamente, la libertà, intesa come indipendenza e autonomia, viene a tradursi in uno spazio di azione proprio, esclusivamente occupato dal soggetto stesso. A. LO

condivisa in cui gli individui si manifestano e prendono parte alla vita collettiva, poiché ciò che emerge in questa sfera assume consistenza proprio grazie al fatto di essere percepito da altri, in una trama di rimandi e riconoscimenti reciproci. In contrapposizione, condurre un'esistenza confinata esclusivamente nel privato equivale a rinunciare a quella dimensione di realtà che deriva dall'essere visti e ascoltati dagli altri. Tale condizione di privazione implica l'assenza di un mondo comune di cose capace di mediare le relazioni tra le persone. Come sottolinea H. Arendt, "*la privazione implicita nella privacy consiste nell'assenza degli altri; in questo caso, ai loro occhi, l'uomo privato non appare, e quindi è come se non esistesse*".

Questa caratteristica intrinseca della sfera privata non va intesa come negazione o svalutazione del suo ruolo, ma piuttosto come espressione della differenza strutturale tra pubblico e privato: ciò che si compie in ambito privato, infatti, rimane privo di conseguenze per gli altri, come se azioni e parole fossero destinate a non avere risonanza nel mondo. La contrapposizione tra le due sfere, pertanto, non implica una volontà di riduzione o assorbimento dell'una nell'altra, ma, al contrario, richiama la necessità di mantenere una distinzione funzionale, riconoscendo a ciascun ambito la propria autonomia e specificità. Tale distinzione rimanda nuovamente alla tradizione greca, nella quale veniva tracciata una chiara separazione tra *idion* e *koinon*, ovvero tra ciò che è proprio e ciò che è comune, distinzione che si traduceva, in termini più ampi, nella differenza tra la dimensione domestica e quella politica della *polis*[39]. In "*Vita Activa"* H. Arendt rifletteva: "*un uomo che vivesse solo una vita privata e che, come lo*

GIUDICE, *Quel diritto di essere lasciati soli*, in *Teoria e Critica della regolazione sociale*, 1, 2017, 7-10.

[39] Per una ricostruzione puntuale del pensiero di Arendt si segnalano: N. MATTUCCI, *Mondo comune e responsabilità politica. Rileggendo la teoria politica di Hannah Arendt*, Macerata, EUM, 2008, 7-191; H. ARENDT, *Vita activa. La condizione umana*, trad. it., Milano, Bompiani, 1964; H. ARENDT, *La vita della mente*, trad. it., Bologna, Il Mulino, 1987; A. ENEGRÉN, *Il pensiero politico di Hannah Arendt*, Milano, FrancoAngeli, 1997.

schiavo, non potesse accedere alla sfera pubblica o che, come il barbaro, avesse scelto di non istituire un tale dominio, non era pienamente umano".

Si ricorda che, anche in epoca successiva, nella società romana, non esisteva la sfera 'privata' come valore in sé o come presidio fondamentale della libertà e integrità personale, poiché la libertà era rappresentata come una prerogativa pubblica, una qualità del cittadino e non attribuibile a qualsiasi individuo[40]: la libertà si viveva e si otteneva con la città e dentro la città[41].

Nel periodo medievale, il termine *privato* acquisì progressivamente il significato di *familiare*. La dimensione privata si radicava soprattutto nella fiducia reciproca che legava i membri dello stesso nucleo, dando vita a un'intensa esperienza comunitaria in cui non trovava posto la figura dell'individuo isolato. Proprio in questo contesto storico si iniziò a delineare l'esigenza di delimitare spazi di intimità, riconoscibili in ambiti diversi – dalla religione alla vita sociale, fino al pensiero personale – anticipando così un'idea di riservatezza sorprendentemente vicina a quella moderna[42]. Secondo M. Bloch, la società feudale era tuttavia caratterizzata da una marcata trasparenza: la vita degli individui si svolgeva quasi interamente sotto gli occhi della comunità. L'intimità e la possibilità di sottrarsi agli sguardi altrui erano riservate a pochi eletti o a coloro che, per scelta o vocazione, si distaccavano dalla vita collettiva, come i mistici, i monaci, i pastori solitari o i fuorilegge. In questo contesto, la privacy non era un diritto comune, ma un

[40] Curiosamente, alcune tecniche volte a garantire la riservatezza delle comunicazioni si svilupparono proprio nel periodo romano. La crittografia era stabilmente utilizzata nella Roma Antica per consegnare messaggi di natura strategico-militare, tant'è che l'idea che due interlocutori dovessero condividere in anticipo un segreto comune per garantire la riservatezza delle proprie comunicazioni ha radici molto antiche. Negli esperimenti di cifratura attribuiti a Giulio Cesare era evidente come la protezione del messaggio si fondasse sulla condivisione preventiva di una chiave, considerata requisito imprescindibile per uno scambio sicuro. A. LUVISON, *La crittografia, uno snodo cruciale per la cybersicurezza*, in *Mondo Digitale*, 2016, 16.

[41] S. AMATO, *Appunti su aidos e privacy*, in *Teoria e Critica della regolazione sociale*, 2017, 1, 13-25.

[42] A. DEMMA, D. ROFFINELLA, *Dilemma del cyberspazio: privacy o condivisione?*, in *Rivista AEIT*, 2023, 110(2), 6-17.

privilegio eccezionale, legato alla separazione dalla comunità e alla marginalità rispetto alla vita quotidiana della società feudale[43].

S. Rodotà[44], a seguito di un'analisi approfondita sotto il profilo politico, giuridico e socioeconomico, evidenzia come le condizioni per l'emersione della privacy quale esigenza meritevole di autonoma tutela abbiano avuto origine con la disgregazione dell'ordine feudale. Eminenti storici sociali hanno individuato, a partire dal XVI secolo, una crescente consapevolezza del valore della privacy individuale in numerosi ambiti della cultura europea. La crescente importanza sociale attribuita al valore della privacy si riflette nei cambiamenti delle pratiche religiose, nelle espressioni artistiche, nelle abitudini alimentari, nell'architettura, nell'abbigliamento. Parallelamente a questi sviluppi culturali, si riscontrano dibattiti giuridici nati nei primi anni del XVI secolo, nonché decisioni dei tribunali di *common law* a partire dal XVII secolo, che mettono in discussione la prassi dei tribunali inquisitori di costringere l'imputato a testimoniare contro sé stesso, l'uso della tortura a fini investigativi e la persecuzione degli individui sulla base di pensieri eretici o traditori. Nello stesso periodo, i giudici iniziano a imporre limiti sempre più rigorosi alla facoltà dei funzionari statali di perquisire le abitazioni private alla ricerca di prove. Verso la metà del XVIII secolo, quando il concetto di una sfera di vita privata era ormai largamente accettato nella società, il giurista Sir W. Blackstone riconosceva come principio giuridico consolidato che i "vizi privati" e le "personali convinzioni o incredulità religiose" non rientrassero nella sfera di competenza del magistrato e, pertanto, non potessero essere oggetto di sanzione[45].

Nel 1766, Lord Chatham si rivolse al Parlamento inglese con parole che sottolineavano il valore della sfera privata anche per i cittadini più poveri.

---

[43] S. RODOTÀ, *Persona, libertà, tecnologia: Note per una discussione*, in *Diritto & Questioni Pubbliche*, 2005, 5, 25-29.
[44] S. RODOTÀ, *La privacy tra individuo e collettività*, in *Politica del Diritto*, 1974, 5, 545.
[45] P. A. WINN, *Older than the Bill of Rights: The Ancient Origins of the Right to Privacy*, 2010.

Egli affermò che, anche nella più modesta abitazione, un individuo può opporsi a qualsiasi abuso del potere reale: "*la casetta può essere fragile, il suo tetto traballante, il vento e la pioggia possono penetrarvi, eppure il Re d'Inghilterra non può entrare; nessuna delle sue forze osa oltrepassare la soglia di tale dimora in rovina*". Con questa dichiarazione, Chatham riconosceva simbolicamente il diritto alla protezione della proprietà privata e alla privacy come limite invalicabile rispetto al potere dello Stato. È noto che proprio l'esigenza di tutelare la proprietà privata, intesa da Locke in senso ampio come comprensiva anche del diritto alla vita e alla libertà, conduce all'istituzione dello Stato, concepito come ente pubblico chiamato non solo a proteggere i diritti dell'individuo da possibili aggressioni, ma anche ad astenersi da indebite interferenze nello spazio privato[46].

La privacy si configura, a partire da questo periodo, come un bisogno sempre più caratteristico della classe borghese emergente, strettamente connesso alle trasformazioni socioeconomiche indotte dalla rivoluzione industriale, le quali contribuirono a ridefinire il rapporto tra individuo e potere, andando ad imporre nuove riflessioni sui limiti dell'intervento statale nella sfera privata[47].

1.2.2 La privacy negli ordinamenti giuridici

Da un punto di vista dottrinale, la nascita del diritto alla privacy viene fatta risalire al 1890, anno in cui i giuristi statunitensi Samuel Warren e Louis Brandeis pubblicarono, nella rinomata *Harvard Law Review*, un saggio intitolato "*The Right to Privacy. The Implicit Made Explicit*"[48]. Il diritto alla privacy, nella sua concezione originale, era accompagnato dalla definizione,

[46] A. LO GIUDICE, *Quel diritto di essere lasciati soli*, in *Teoria e Critica della regolazione sociale*, 1, 2017, 7-10.
[47] V. COLOMBA, G. ZANETTI, *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in *Teoria e Critica della regolazione sociale*, 2017, 1, 27-39.
[48] S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, 4(5).

attribuita al giudice statunitense T. Cooley: "*the right to be let alone*" (il diritto di essere lasciati soli). In un contesto sociale in evoluzione, segnato dal recente sviluppo tecnologico e dall'introduzione delle macchine da stampa a rotativa e delle macchine fotografiche (che consentivano alla stampa scandalistica statunitense di corredare gli articoli con le foto degli interessati) emerse l'esigenza di definire un diritto volto a eliminare le intrusioni nella propria vita privata. L'occasione per la formulazione e l'enunciazione del *right to privacy* si presentò a seguito di un episodio verificatosi negli Stati Uniti in quel periodo. La vicenda, ampiamente nota, merita di essere brevemente richiamata anche in considerazione della sua attualità. Samuel Warren, avvocato di origine bostoniana, dopo aver contratto matrimonio con la figlia del facoltoso Byard, intraprese una vita sociale caratterizzata da ricevimenti sfarzosi, analoghi a quelli che, una generazione più tardi, sarebbero stati resi celebri nei romanzi di F. Scott Fitzgerald. L'attenzione della stampa locale si concentrò su tali eventi mondani, enfatizzandone il lusso e formulando giudizi critici su tali ostentazioni.

Di fronte all'invadenza della stampa, Warren si associò al collega Louis Brandeis – futuro giudice della Corte Suprema – con il quale redasse un articolo destinato a divenire un pilastro della dottrina giuridica e promosse un'azione legale volta a ottenere il riconoscimento del diritto alla riservatezza. L'obiettivo non era tanto la tutela della solitudine fisica, quanto piuttosto l'affermazione della privacy quale presidio giuridico dell'autonomia e della dignità dell'individuo, comprensivo della protezione della sua sfera familiare e delle relazioni sociali liberamente intraprese[49].

Il saggio ebbe un impatto significativo sulla giurisprudenza e sulle leggi relative alla privacy negli Stati Uniti, contribuendo a gettare le basi per il riconoscimento del diritto alla privacy come parte integrante dei diritti

[49] T. E. FROSINI, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, 2022, 51(1), 273-284.

individuali. Il riferimento risulta di particolare interesse per l'attenzione che gli autori riservano alle macchine e, dunque, alla tecnologia: "…*numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops*'". Essi costatano quindi l'intrusione, non solo della stampa, ma anche degli strumenti tecnologici all'interno della sfera privata e domestica dell'individuo, con l'effetto di produrre un effetto "sorveglianza". Gli autori hanno infatti contribuito a sostenere l'idea che debba spettare all'individuo determinare "*to what extent his thoughts, sentiments, and emotions shall be communicated to others*".

In mancanza di un riferimento normativo esplicito nella Costituzione federale statunitense o in altre fonti legislative riguardo alla privacy, i due autori individuano nella giurisprudenza (*common law*) la fonte del diritto in materia[50]. Con la teorizzazione di Warren e Brandeis, si è assistito a una trasformazione degli strumenti di protezione della riservatezza. La privacy non è più considerata un semplice effetto secondario della tutela del diritto sulla *res*, ma si è affermata come un diritto autonomo, riconducibile quindi ai diritti fondamentali dell'individuo, tutelando così la persona nella sua interezza[51].

I tribunali americani, già prima della pubblicazione del saggio di Warren e Brandeis, avevano riconosciuto l'importanza di proteggere la privacy personale, da un punto di vista giuridico, in contesti disparati: le dottrine relative alla violazione di domicilio, alle intercettazioni, alla diffamazione, alla perquisizione e al sequestro irragionevoli, alla riservatezza della corrispondenza e delle informazioni ottenute tramite censimento rientravano tra le casistiche affrontate dai tribunali statali e federali per

[50] R. CASO, *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Milano, Ledizioni, 2021, 1-364.
[51] F. BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Il diritto dell'informazione e dell'informatica*, 2023, 3, 481-518.

tutelare quella che esplicitamente definivano la "privacy" dell'individuo. Warren e Brandeis auspicavano che i tribunali elevassero questa protezione esistente a un livello di garanzie superiori, al fine di impedire la pubblicazione di informazioni di natura personale (in particolare di fotografie) sulla stampa quotidiana. Poco prima di Warren e Brandeis, un editore di una rivista americana aveva definito l'interesse per la privacy in termini più ampi come "*il valore attribuito... al potere di tracciare, ciascuno per sé, la linea di demarcazione tra la sua vita di individuo e la sua vita di cittadino*", o in altre parole, "il potere di decidere quanto o quanto poco la comunità dovrà vedere di lui, o sapere di lui", andando ad anticipare una certa coscienza relativa all'autodeterminazione informativa[52].

Si nota, dunque, come, a distanza di oltre un secolo, le riflessioni e le problematiche emerse siano tuttora attuali, anche applicate al contesto tecnologico contemporaneo. È indubbio che, a partire dagli anni '70 del secolo scorso, siano state in particolare le tecnologie informatiche a determinare un significativo avanzamento nell'evoluzione del diritto in questione. Con l'introduzione delle prime banche dati, infatti, si delinea un aspetto fino ad allora inedito: la tutela dei dati personali, intesa come il diritto, da parte dell'interessato, di esercitare un controllo sull'utilizzo che terzi fanno delle proprie informazioni[53].

Questo fenomeno conferma pertanto la tesi di N. Bobbio, secondo cui i diritti hanno un fondamento storico e si sviluppano e si evolvono in concomitanza con i mutamenti storici, economici e sociali[54]. Il diritto alla privacy, infatti, nasce come un'esigenza della comunità borghese statunitense di fine Ottocento e si afferma come diritto giuridico in epoca moderna,

[52] D. J. SEIPP, *English judicial recognition of a right to privacy*, in *Oxford Journal of Legal Studies*, 1983, 3, 328.
[53] S. SCAGLIARINI, *Identità digitale e tutela della privacy*, in *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, atti del convegno, Genova, 18-19 giugno 2021, in *Quaderni del Gruppo di Pisa*, 2022.
[54] N. BOBBIO, *L'età dei diritti*, Torino, Einaudi, 1990.

trasformandosi in un diritto esigibile grazie alla disciplina stabilita da specifiche leggi, sebbene ciò sia avvenuto in Stati e periodi diversi.

Come accennato, trattando il termine *privacy* inizialmente si è fatto riferimento al diritto alla riservatezza, per poi giungere, in particolar modo dopo l'avvento della rete Internet, al diritto alla protezione dei dati personali. Questo perché, attraverso il fenomeno dell'*Internet of Things*, alla nostra identità di persone fisiche si è aggiunta una seconda identità virtuale, caratterizzata dalle nostre attività in rete e dalle tracce che lasciamo durante la fruizione di beni e servizi collegati alla rete stessa, producendo un enorme quantitativo di dati che riguardano le nostre scelte e delineano la nostra persona. Quella che inizialmente era una dipendenza dai dati, tipica delle macchine (*data dependency*), si è progressivamente trasformata in una nostra dipendenza dalle macchine stesse e, di conseguenza, dallo sfruttamento dei dati a nostro vantaggio (*data dependencies*). Oggi facciamo affidamento sulla circolazione di dati e di informazioni per il normale esercizio della nostra personalità, sia a livello individuale che all'interno delle nostre cerchie sociali. Le implicazioni della dipendenza dai dati sono molteplici, e segnano il passaggio dalla visione ottimistica dell'innovazione guidata dai dati (*data-driven innovation*) a una più stringente dipendenza sistematica e strutturale dalla datificazione, ponendo così una questione di diritto costituzionale[55]. A tal riguardo, secondo S. Rodotà, "*il corpo elettronico e la sua gestione rimangono nella sfera giuridica della persona*", poiché la disciplina per la protezione dei dati offre tutele ma anche diritti per esprimere la volontà rispetto all'utilizzo dei dati che lo riguardano e sono a lui riconducibili[56].

Quando si discute dell'effettività dei diritti costituzionalmente riconosciuti, occorre considerare la finalità di sviluppo della personalità

[55] S. CALZOLAIO, *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in *Rivista Italiana di Informatica e Diritto*, 2024, 5(2), 13-33.
[56] S. MARTINELLI, *I nuovi modelli per l'utilizzo dei dati: digital services e data economy*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024.

dell'individuo, come previsto dall'art. 2 Cost., anche nella sua dimensione sociale, nonché la promozione di tali diritti in termini di pari dignità sociale e di uguaglianza formale e sostanziale ai sensi dell'art. 3 Cost. In questo quadro, tali principi trovano oggi nuova espressione nella dimensione digitale dell'esistenza, segnata dal tempo che ciascun individuo trascorre sul web.

È opportuno sottolineare come, mediante l'utilizzo di un fondamentale servizio – il protocollo informatico – sia possibile esercitare pressoché tutti i diritti di libertà costituzionalmente tutelati, con modalità analoghe a quelle ordinarie. Tuttavia, tali modalità spesso producono effetti che, semplificando, possono essere qualificati come potenziati, sia in positivo sia in negativo, incidendo quindi sulla concreta realizzazione dei diritti stessi nell'ambiente digitale[57].

Si sottolinea nuovamente come il diritto alla privacy abbia infatti subito un'evoluzione significativa nel corso del tempo. Inizialmente, esso era concepito come un diritto alla riservatezza, e quindi limitato alla protezione delle informazioni personali da intrusioni esterne. Tuttavia, con l'avvento delle tecnologie digitali e l'espansione dell'economia dell'informazione, il concetto di privacy si è ampliato notevolmente. Attualmente, il diritto alla privacy include non solo il diritto alla riservatezza, ma anche un più ampio diritto al controllo sui propri dati personali. Si parla ora di *informational privacy*, un concetto che riflette la complessità e l'interconnessione della privacy con l'economia dell'informazione. L'*informational privacy* si riferisce alla tutela delle informazioni personali nel quadro delle attività economiche e tecnologiche moderne, dove i dati rappresentano una risorsa fondamentale[58]. Grazie all'intelligenza artificiale, tutti i tipi di dati personali possono essere utilizzati per analizzare, prevedere e influenzare quello che sarà il

[57] P. MARSOCCI, S*empre "al lavoro". Le garanzie costituzionali di persone e personalità connesse in Rete*, in *Rivista italiana di informatica e diritto*, 2021, 2, 73-88.
[58] C. FARALLI*, Il diritto alla privacy. Profili storico-filosofici*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. ZORZI GALGANO, Milano, Cedam – Wolters Kluwer, 2019, 1-7.

comportamento umano, ed assumono così il carattere di merci di valore. Informazioni che un tempo non venivano per nulla raccolte od erano considerate scarti (i cosiddetti "dati di scarto" o "*exhaust data*") sono ora diventate una risorsa preziosa[59].

Nell'attuale sistema economico e sociale, le attività pubbliche e private sono sempre più frequentemente affidate a Internet e all'informatica (e con questa si intendono anche gli algoritmi). Ciò ha comportato un cambiamento radicale nella gestione dei dati, portando ad una "mercificazione delle informazioni". Non facciamo più riferimento soltanto alle informazioni personali di interesse per la cronaca (come ai tempi di Warren e Brandeis), ma ad un ampio spettro di dati, comprese quelle informazioni che, se prese singolarmente, possono apparire di scarso significato. Tuttavia, quando queste informazioni vengono aggregate e analizzate, acquisiscono un valore. I dati trattati, che riguardano ogni aspetto della vita di ciascuno di noi, vengono sistematicamente raccolti e fatti circolare all'interno di un complesso ecosistema digitale composto da algoritmi, banche dati, motori di ricerca e social network e, per questa ragione, tale evoluzione ha spostato quello che era il focus primario delle intrusioni nella vita privata. Da una prospettiva soggettiva, tali intrusioni non derivano più principalmente dai mezzi di informazione tradizionali, ma dall'uso pervasivo e spesso invisibile dei dati personali da parte di operatori economici e altre entità. Questo utilizzo diffuso e sofisticato dei dati personali solleva preoccupazioni significative riguardo alla privacy e al controllo delle informazioni. In tale contesto, emerge un interesse nel conoscere come i dati vengano raccolti, utilizzati e condivisi. La consapevolezza e la gestione di queste dinamiche diventano quindi fondamentali per tutelare i diritti individuali e garantire un equilibrio tra l'innovazione tecnologica e la

[59] F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 2020, 11, 85-110.

protezione dei dati personali. In termini strutturali, come osservato da V. Cuffaro, si assiste alla progressiva sostituzione del modello tradizionale del diritto alla riservatezza, fondato sull'individuazione di un bene riconducibile al soggetto e sulla conseguente tutela in caso di violazione secondo il paradigma della responsabilità da fatto illecito. Al suo posto, viene adottato un modello che si focalizza sulla relazione tra chi fornisce e chi utilizza i dati personali, seguendo il paradigma del rapporto obbligatorio. Questo approccio richiama il principio della correttezza nel trattamento dei dati e il bilanciamento degli interessi delle parti coinvolte nel rapporto. In termini sostanziali, si contrappongono due profili relativi alle informazioni sulla persona: da un lato, l'informazione che viene raccolta inizialmente e poi diffusa, trasformandosi in notizia; dall'altro lato, le informazioni che la persona stessa fornisce e che vengono trattate attraverso sistemi informatici, più o meno consapevolmente, diventando oggetto di un trattamento[60].

Come accennato, a partire dagli anni Settanta, si assiste all'inarrestabile diffusione dei personal computer e, con l'avvento degli anni Novanta, del *World Wide Web*. L'accessibilità a vastissime banche dati e l'incremento esponenziale della capacità computazionale sollecitano i legislatori nazionali a promulgare normative atte a disciplinare il trattamento dei dati, coinvolgendo ineluttabilmente le esistenze degli individui. Si inaugura così la storia della disciplina riguardante la protezione dei dati personali[61].

L'attenzione della dottrina italiana verso la riservatezza trova un riferimento centrale nell'opera di A. De Cupis[62], che la incluse tra i diritti della personalità, intesa come tutela dalla presenza invasiva di terzi nella sfera

[60] V. CUFFARO, *Il diritto europeo sul trattamento dei dati e la sua applicazione in Italia: elementi per un bilancio ventennale*, in *I dati personali nel diritto europeo*, V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, Giappichelli, 2019, 3-17.
[61] P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, Milano, Ledizioni, 2023.
[62] A. DE CUPIS, *I diritti della personalità*, 2ª ed. riveduta e aggiornata, Milano, Giuffrè, 1926.

privata dell'individuo. Il percorso di riconoscimento del diritto all'identità personale ha trovato invece un primo compiuto riconoscimento giurisprudenziale soltanto nel 1985, grazie a una significativa pronuncia della Corte di cassazione[63]. In tale occasione, la Corte affrontò organicamente la questione, delineandone i tratti essenziali sulla base di posizioni già maturate nella giurisprudenza di merito e nella dottrina dominante. Da questa evoluzione emerge una chiara distinzione: la figura di riferimento non è più l'uomo considerato come individuo isolato, bensì come soggetto inserito nella rete delle relazioni sociali, in cui la sua immagine acquista rilevanza pubblica e significato collettivo. La questione è stata affrontata dal legislatore italiano in maniera frammentaria, attraverso disposizioni sparse nella Costituzione. Si possono rinvenire riferimenti indiretti alla protezione della sfera privata, ad esempio nella tutela del domicilio (art. 14), nella garanzia della libertà e segretezza della corrispondenza (art. 15) e nella libertà di espressione del pensiero (art. 21). Inoltre, come accennato, un fondamento più ampio e implicito si può ricavare dall'articolo 2 della Carta costituzionale, che riconosce e garantisce i diritti inviolabili della persona[64].

[63] La prima pronuncia di rilievo in materia è rappresentata dalla sentenza della Corte di cassazione n. 3769 del 22 giugno 1985, preceduta dalla decisione del Tribunale di Roma del 10 marzo 1982. In tale occasione, la Suprema Corte ha affermato che ogni individuo ha un interesse, riconosciuto come meritevole di tutela giuridica, a essere rappresentato nella vita di relazione secondo la propria effettiva identità, così come questa è conosciuta, o può essere conosciuta, nella realtà sociale, generale o particolare, secondo criteri di normale diligenza e di buona fede soggettiva. L'interesse tutelato si sostanzia, pertanto, nel diritto del soggetto a non vedere alterato, travisato, offuscato o contestato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, ideologico o professionale, quale si è manifestato o appare destinato a manifestarsi nell'ambiente sociale, in base a circostanze concrete e univoche. A. RANDAZZO, *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in *Dirittifondamentali.it*, 2021, 3, 370-371.
[64] M. IASELLI, V. IASELLI, *Nuove tecnologie, sicurezza e protezione dei dati*, Milano, Giuffrè Francis Lefebvre, 2024.

1.3 Il diritto alla protezione dei dati personali nell'ordinamento dell'Unione Europea

1.3.1 La normativa europea in materia di privacy antecedente al 'nuovo' "Pacchetto Protezione Dati"

In Europa, il percorso verso un impiego responsabile delle nuove tecnologie ha preso avvio già da diversi anni, in seguito all'esperienza statunitense, iniziata molto tempo prima (proprio negli Stati Uniti si colloca l'origine del diritto alla riservatezza), sebbene già nell'Inghilterra di fine Ottocento si possano rintracciare i primi germogli di tale disciplina. Tra i casi rimasti celebri, si ricorda "*Prince Albert vs Strange*": era il 1848 quando un dipendente della Corte britannica riuscì a realizzare, con l'intento di divulgarle, copie non autorizzate di alcune acqueforti commissionate dalla regina Vittoria e dal principe Alberto per raffigurare i loro figli. Da quel momento in poi, le corti inglesi hanno generalmente fatto applicazione della cosiddetta *breach of confidence rule*, fondata essenzialmente su tre elementi: la natura confidenziale dell'informazione, l'obbligo di riservatezza e l'utilizzo non autorizzato del contenuto divulgato[65].

La nozione di dato personale tuttavia si afferma successivamente, e rappresenta uno degli istituti centrali introdotti dalla Convenzione di Strasburgo n. 108 del 28 gennaio 1981, intitolata *Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*[66]. Lo scopo di tale Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua

[65] A. ALONGI, F. POMPEI, *Diritto della privacy e protezione dei dati personali – Il GDPR alla prova della data driven economy*, Roma, Tab Edizioni, 2021, 13-15.

[66] Tale Convenzione non assume la denominazione di Convenzione europea, affinché possano aderire anche Stati non facenti parte del Consiglio d'Europa, come descritto dall'art.23 della stessa: "*Dopo l'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa potrà invitare qualsiasi Stato non membro del Consiglio d'Europa ad aderire alla presente Convenzione mediante una decisione presa con la maggioranza prevista dall'articolo 20 lettera d dello Statuto del Consiglio d'Europa ed all'unanimità dei rappresentanti degli Stati contraenti aventi diritto di sedere al Comitato*".

nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano. In base a quanto disposto dall'articolo 2, per "dati a carattere personale" sono da intendersi ogni informazione concernente una persona fisica identificata o identificabile ("persona interessata")[67].

Nel contesto europeo il diritto al rispetto della vita privata e familiare, è fondato sull'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU[68]); l'art. 9 CEDU riconosce invece il diritto alla libertà di pensiero, di coscienza e di religione; mentre l'art. 10 assicura la libertà di opinione e di ricevere o comunicare informazioni e l'art. 11 consacra la libertà di riunione e di associazione[69]. L'enunciato dell'art. 8 della CEDU è ribadito nell'articolo 7[70] della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza)[71], che riveste un'importanza fondamentale nel contesto giuridico europeo. L'articolo 8 della CEDU garantisce il diritto al rispetto della vita privata, familiare, del domicilio e della corrispondenza, sancendo che nessuna interferenza può avvenire nell'esercizio di tale diritto se non in conformità con la legge e quando necessaria in una società democratica per motivi di sicurezza nazionale, sicurezza pubblica, benessere economico del paese, prevenzione del disordine o del crimine, protezione della salute o della morale, o protezione dei diritti e delle libertà altrui.

---

[67] C. SPINIELLO, *ScheDati. Il diritto alla protezione dei dati personali nella legislazione europea*, in *Democrazia e Sicurezza*, 8(1), 2018, 143–188.

[68] Firmata nel 1950 dal Consiglio d'Europa, la convenzione è un trattato internazionale volto a tutelare i diritti umani e le libertà fondamentali in Europa.

[69] L. BEDUSCHI, *La giurisprudenza di Strasburgo 2008-2010: gli altri diritti di libertà (artt. 8-11 CEDU)*, in *Diritto penale contemporaneo – Rivista trimestrale*, 2011, 1, 289-322.

[70] *"Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."*

[71] Essa pone la persona al centro della sua azione istituendo la cittadinanza dell'Unione e creando uno spazio di libertà, sicurezza e giustizia.

L'articolo 7 della Carta di Nizza, invece, reitera questi principi fondamentali, garantendo la loro applicazione diretta all'interno dell'ordinamento giuridico dell'Unione Europea. Questo significa che tali diritti devono essere rispettati e tutelati in tutte le attività normative e decisionali dell'Unione Europea e dei suoi Stati membri, incluso il trattamento dei dati personali e la regolamentazione della privacy nell'ambito digitale e non.

La salvaguardia del diritto al rispetto della vita privata e familiare, pertanto, rappresenta un pilastro essenziale della protezione dei diritti fondamentali dell'Unione Europea, garantendo ai cittadini europei una difesa robusta e conforme ai principi democratici e costituzionali sia a livello nazionale che sovranazionale[72]. Accanto a ciò, è essenziale evidenziare diverse direttive e normative che hanno sostenuto e consolidato il diritto al rispetto della vita privata e familiare nell'Unione Europea. Inizialmente, le seguenti direttive hanno assunto un ruolo fondamentale:

- La Direttiva 95/46/CE[73], relativa alla tutela delle persone fisiche per quanto riguarda il trattamento dei dati personali e la libera circolazione di tali dati all'interno dell'Unione Europea, ha introdotto principi significativi per la protezione dei dati personali.
- La Direttiva 97/66/CE[74] ha ulteriormente sviluppato le disposizioni sulla protezione dei dati personali nel settore delle telecomunicazioni, rafforzando la sicurezza e la privacy delle comunicazioni.

[72] E. CREMONA, *Quando i dati diventano beni comuni: Modelli di data sharing e prospettive di riuso*, in *Rivista Italiana di Informatica e Diritto*, 2024, 5(2), 111-130.
[73] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati. *Gazzetta ufficiale dell'Unione europea*.
[74] Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni. *Gazzetta ufficiale dell'Unione europea*.

- La Direttiva 2002/58/CE[75], "relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche", nota come "Direttiva sulla privacy elettronica", ha esteso le normative sulla protezione dei dati personali al contesto delle comunicazioni elettroniche, affrontando le sfide specifiche del settore digitale.

Successivamente, l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza nel 2000, ha attribuito al diritto al rispetto della vita privata e familiare lo stesso valore giuridico dei Trattati dell'Unione, elevandolo così a principio di rango costituzionale. Parallelamente, l'articolo 16[76] del Trattato sul Funzionamento dell'Unione Europea (TFUE) ha ulteriormente consolidato questi principi, stabilendo la protezione dei dati personali come elemento fondamentale della politica dell'Unione Europea.

Tra le disposizioni oggetto di analisi, è indubbio che l'art. 8 della Carta[77] rappresenti l'innovazione più rilevante. Sebbene le Spiegazioni allegate alla Carta abbiano cercato di ridurne la portata a una semplice riproposizione dell'acquis esistente, l'art. 8 introduce cambiamenti

[75] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva sulla vita privata e le comunicazioni elettroniche). *Gazzetta ufficiale dell'Unione europea*.

[76] "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea.*"

[77] "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*"

significativi. Non solo costituzionalizza il diritto alla protezione dei dati personali, ma lo emancipa definitivamente dalla sua originaria connessione con la dimensione economica legata al consolidamento del mercato interno, come previsto nella direttiva 95/46[78]. Con l'entrata in vigore del Trattato di Lisbona del 2007, che ha conferito carattere vincolante alla Carta di Nizza, questa tutela è stata estesa anche all'art. 16 TFUE ("Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano"). Tuttavia, come sottolineato, va riconosciuto che già l'art. 8 della Carta, fin dal 2001, aveva assunto un ruolo pionieristico in questo contesto, costituendo un punto di riferimento fondamentale e attribuendo al Garante per la protezione dei dati personali un riconoscimento costituzionale unico tra le autorità indipendenti[79].

La Corte Europea dei Diritti dell'Uomo di Strasburgo ha emesso diverse sentenze rilevanti in materia di protezione della riservatezza, intesa come tutela della vita privata dell'individuo anche in contesti pubblici. In

[78] Al considerando n.2 della direttiva è riportato: "*considerando che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui";* mentre al considerando n.3 della stessa: *"considerando che l'instaurazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 7 A del trattato, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona."* La direttiva, al considerando n.8, introduceva una problematica affrontata poi dal GDPR: "*considerando che, per eliminare gli ostacoli alla circolazione dei dati personali, il livello di tutela dei diritti e delle libertà delle persone relativamente al trattamento di tali dati deve essere equivalente in tutti gli Stati membri; che tale obiettivo, fondamentale per il mercato interno, non può essere conseguito esclusivamente attraverso l'azione degli Stati membri, tenuto conto in particolare dell'ampia divergenza esistente attualmente tra le normative nazionali in materia e della necessità di coordinarle affinché il flusso transfrontaliero di dati personali sia disciplinato in maniera coerente e conforme all'obiettivo del mercato interno ai sensi dell'articolo 7 A del trattato; che risulta pertanto necessario un intervento della Comunità ai fini di un ravvicinamento delle legislazioni*".

[79] O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai Giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di G. RESTA, V. ZENO-ZENCOVICH, 2015, 7-28.

particolare, casi significativi come *Von Hannover v. Germania* (24 settembre 2004, no. 59320/00) e *Axel Springer v. Germania* (7 febbraio 2012, no. 39954/08) hanno enfatizzato il concetto di "ragionevole aspettativa di riservatezza", stabilendo che anche in situazioni pubbliche, gli individui possono legittimamente aspettarsi una protezione adeguata della propria vita privata. La Corte si è pronunciata anche sulla protezione del segreto nelle comunicazioni e sulle intercettazioni. Ad esempio, nei casi *Malone v. Regno Unito* (2 agosto 1984, no. 8691/79) e *Huvig v. Francia* (24 aprile 1990, no. 11105/84)[80].

Più recentemente, tra il 2014 e il 2015, i giudici comunitari della Corte di giustizia dell'Unione europea (CGUE) hanno emesso tre decisioni che rivelano chiaramente la loro intenzione di prendere molto seriamente la protezione di un nuovo diritto alla privacy digitale. Questo impegno si è manifestato in un approccio che va oltre il mero formalismo, garantendo un elevato livello di tutela degli articoli 7 e 8 della Carta. Tale protezione è stata assicurata anche a scapito di altri diritti di pari rango, come la libertà di espressione.

Il processo può essere semplificato richiamando tre decisioni fondamentali. La prima è il caso *Digital Rights Ireland*[81], in cui i giudici di Lussemburgo hanno annullato la direttiva 2006/24[82] sulla conservazione dei dati perché in contrasto con la Carta dei diritti fondamentali dell'Unione Europea[83].

---

[80] P. GUARDA, G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, Milano, Ledizioni, 2023.

[81] CGUE, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, 2014.

[82] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante 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 e che modifica la direttiva 2002/58/CE, in *Gazzetta ufficiale dell'Unione europea.*

[83] O. POLLICINO e M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, a cura di G. RESTA e V. ZENO-ZENCOVICH, Roma, Roma Tre Press, 2016, 73-92.

La seconda è il caso *Google Spain*[84], dove la Corte ha stabilito che, in certe condizioni, i motori di ricerca devono rimuovere, su richiesta, link a pagine Internet contenenti informazioni che possano ledere il diritto all'oblio di una persona. In questa circostanza la Corte ha chiarito come i diritti fondamentali di cui agli artt. 7 e 8 della Carta "prevalgono, in linea di principio, sull'interesse economico" del gestore del motore di ricerca[85].

Infine, il caso *Schrems*[86] ha visto la Corte invalidare la decisione della Commissione Europea che, nel 2000, aveva approvato i principi del *Safe Harbor* per il trasferimento dei dati personali tra Europa e Stati Uniti. La decisione della Corte di Giustizia nel caso *Schrems c. Data Protection Commissioner* può essere vista, se non come un *leading case*, sicuramente come uno dei precedenti più influenti nella giurisprudenza europea recente in materia di diritti fondamentali[87]. Un passaggio specifico della pronuncia in esame sembra evidenziare nuovamente un approccio interpretativo della Corte caratterizzato da una certa espansività, quasi manipolativa, delle disposizioni della direttiva. Tale interpretazione, presumibilmente volontaria, sembra mirare a garantire una tutela più ampia possibile dei dati personali. La Corte attribuisce all'art. 25, comma 6[88], della Direttiva 95/46, che conferisce alla Commissione il potere di valutare l'adeguatezza della protezione dei dati offerta da un paese terzo, l'obiettivo di assicurare una continuità, quasi un'estensione spaziale della protezione giuridica, del livello elevato di tutela

---

[84] CGUE, C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González* (2014).
[85] P. STANZIONE, *Conclusioni*, in A. MORACE PINELLI, *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, Pisa, Pacini Giuridica, 2024, 125-130.
[86] CCGUE, C-362/14, *Maximillian Schrems c. Data Protection Commissioner* (2015).
[87] G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il Diritto dell'Informazione e dell'Informatica*, 2015, 697-718.
[88] *"La Commissione può constatare, secondo la procedura di cui all' articolo 31 , paragrafo 2 , che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5 , ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona."*

previsto all'interno dell'Unione Europea. Anche in questo caso, la Corte sembra aver aderito a questo approccio interpretativo, continuando a perseguirlo[89].

Sebbene trattino temi diversi, ciascuna di esse contribuisce in modo rilevante a ridefinire lo statuto dei dati personali nell'epoca dei big data e della "sorveglianza liquida"[90]. Anche se inizialmente possano sembrare distinti e privi di collegamenti, i tre casi condividono due elementi fondamentali: la dimensione digitale, con la sua prospettiva transnazionale, e la necessità di assicurare una protezione elevata della privacy e dei dati personali come diritti fondamentali, soprattutto contro i nuovi poteri privati del web. Non è un caso che in queste situazioni la Corte abbia garantito un'ampia tutela di tali diritti, estendendone i confini. I giudici di Lussemburgo sono giunti a queste conclusioni attraverso un'interpretazione creativa del diritto derivato alla luce degli articoli 7 e 8 della Carta, che costituiscono il fondamento della protezione della privacy digitale. I casi esaminati dalle Corti evidenziano che, in alcune situazioni, può sorgere un conflitto tra la necessità di proteggere i dati personali e quella di garantire la sicurezza. Tuttavia, è importante sottolineare che le decisioni delle Corti, sia a Strasburgo che in Lussemburgo, sfatano la semplificazione che oppone "privacy" a "sicurezza". Al contrario, queste sentenze dimostrano che è possibile e necessario raggiungere un equilibrio tra le due esigenze, assicurando che nessuna delle due venga compromessa e, in particolare, tutelando il nucleo essenziale del diritto individuale alla protezione dei dati personali[91].

---

[89] O. POLLICINO e M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, a cura di G. RESTA e V. ZENO-ZENCOVICH, Roma, Roma Tre Press, 2016, 73-92.

[90] Secondo la suggestiva formulazione di Bauman e Lyon , il concetto di sorveglianza liquida offre una nuova prospettiva su quelle che sono le dinamiche odierne della sorveglianza sociale. Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Bari, Laterza, 2014.

[91] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Media Laws*, 2018, 2, 82-104.

Nonostante la lettura letterale dell'articolo 51 della Carta possa implicare una restrizione nell'applicazione dei diritti fondamentali nei rapporti tra privati, l'analisi fin qui condotta evidenzia chiaramente come la Corte, in determinati contesti, abbia dimostrato la volontà di andare oltre questa interpretazione testuale per garantire una protezione effettiva dei diritti fondamentali nell'ambito del quadro costituzionale europeo. Questo aspetto è particolarmente evidente nel campo della privacy e della protezione dei dati nel contesto digitale, ambito in cui la Corte di giustizia ha svolto un ruolo centrale garantendo una tutela estesa dei diritti fondamentali, superando i limiti letterali e formali imposti dalla Carta. Alla luce di quanto precedentemente esposto, sembra quindi possibile concludere che, nonostante il ritardo di alcuni anni, la ritrovata vocazione costituzionale della Corte di Giustizia abbia aperto la via a una tutela completa del diritto alla riservatezza e alla protezione dei dati personali[92].

1.3.2 Il Regolamento UE 2016/679 (General Data Protection Regulation)

L'ordinamento giuridico europeo, dopo un lungo percorso che ha portato al formale riconoscimento del diritto alla protezione dei dati personali nell'ambito della Carta dei diritti fondamentali dell'UE (con il già citato art. 8), il 27 aprile 2016, si è arricchito grazie all'approvazione del Regolamento UE 2016/679 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), meglio conosciuto come "GDPR", acronimo di "*General Data Protection Regulation*".

[92] F. VECCHIO, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, 2014, 4, 212-220.

La privacy digitale diventa in questo momento una realtà concreta. Il 25 maggio 2018 è una data emblematica, poiché segna l'effettiva entrata in vigore della nuova regolamentazione uniforme riguardante la tutela della riservatezza e la protezione dei dati personali delle persone fisiche. L'introduzione di questa rilevante normativa ha comportato la necessità di armonizzare il Codice Privacy, un compito realizzato mediante il Decreto Legislativo 10 agosto 2018, n. 101, entrato in vigore il 19 settembre 2018. Questa armonizzazione è stata fondamentale per garantire la protezione dei diritti fondamentali alla riservatezza e alla protezione dei dati personali, sanciti dall'articolo 2 della Costituzione italiana e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea.

Si è profilato un mutamento di rilievo nel panorama economico-giuridico, caratterizzato dal superamento del precedente sistema incentrato sull'armonizzazione e sull'attuazione mediante normative nazionali, a favore di un Regolamento di immediata e uniforme applicazione in tutti gli Stati membri. Tale strumento normativo ha introdotto disposizioni certe e vincolanti, volte a disciplinare non solo fenomeni non considerati dalla Direttiva 95/46/CE, ma anche a regolamentare le problematiche future connesse allo sviluppo del Mercato Unico Digitale[93].

Il GDPR, con la sua natura intrinsecamente transnazionale, è in grado di fungere da punto di riferimento normativo globale, particolarmente efficace nel contesto dinamico e complesso dei mercati digitali. Il Regolamento segna una svolta significativa nella protezione della privacy, rappresentando non solo la conclusione di una lunga battaglia ma anche l'inizio di una nuova e più complessa fase nella difesa dei nostri dati personali, che si trovano dispersi nel vasto mondo virtuale creato dal web. Il testo

[93] A.G. PARISI. *Il regolamento generale sulla tutela dei dati personali. Responsabilità e sanzioni*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G. M. RICCIO, Padova, CEDAM, 2016, 289-311.

normativo riconosce esplicitamente che "*la portata della condivisione e della raccolta di dati personali è cresciuta in modo sostanziale. Le attuali tecnologie consentono sia alle imprese private che alle autorità pubbliche di utilizzare dati personali in modi senza precedenti nel loro svolgimento delle attività*". Questa evoluzione impone una costante vigilanza e adattamento delle normative per affrontare le sfide sempre più complesse poste dalla digitalizzazione dei dati personali.

Il GDPR, nei suoi Considerando, sottolinea come principio generale che "*la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamenta*le". Questo principio riflette il riconoscimento giuridico del diritto alla protezione dei dati personali come parte integrante dei diritti fondamentali delle persone. Inoltre, il regolamento afferma che "*i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali*". Questa disposizione sottolinea l'importanza di garantire che le attività di trattamento dei dati personali non compromettano i diritti e le libertà delle persone. È innegabile che la protezione dei dati personali e la tutela della riservatezza costituiscano valori fondamentali, aventi sia una dimensione fattuale sia una dimensione giuridica. Tuttavia, negli ultimi anni, il fenomeno dei *Big Data* ha portato a un'urgente necessità di riconsiderare questi concetti, poiché la raccolta, l'elaborazione e l'utilizzo massiccio di dati personali possono mettere a rischio il concetto tradizionale di riservatezza come lo abbiamo conosciuto fino ad oggi[94].

Il GDPR mira quindi ad armonizzare le leggi sulla privacy dei dati in tutta l'Unione Europea, garantendo un approccio coerente alla protezione dei dati personali. Quanto descritto è fondamentale per facilitare il libero flusso

[94] E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019.

di dati all'interno del mercato unico europeo[95]. Il regolamento si occupa di riconoscere i diritti fondamentali degli interessati, tra cui il diritto di essere informati rispetto a un trattamento di dati personali, il diritto di accesso, il diritto alla rettifica, il diritto all'oblio e il diritto alla portabilità dei dati. Gli interessati, grazie al regolamento, acquisiscono maggiore controllo sui propri dati personali. Questa serie di diritti comporta che le organizzazioni che trattano dati personali debbano dimostrare la loro conformità al regolamento. Questa viene garantita, per esempio, quando viene formulata la necessaria documentazione delle attività di trattamento, tramite la nomina di un responsabile della protezione dei dati e con la corretta gestione delle violazioni dei dati (data breach)[96].

[95] È interessante notare come nel suo preambolo (al considerando n.4), il GDPR indica che: "*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.*" Tra i diritti fondamentali rientra infatti anche la libertà di impresa, lo stesso regolamento, all'articolo 1 comma n.3 descrive: "*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali."* Il considerando n. 6 procede indicando una certa limitazione al diritto soggettivo, allontanando il diritto alla protezione dei dati personali da un valore considerato assoluto: "*l'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro."* Per questo motivo, alla protezione delle persone fisiche deve accompagnarsi anche la rimozione di quegli ostacoli che possono intercorrere: "*circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri"* (considerando n.10). Come limite all'autonomia privata, tuttavia, entra in gioco l'art. 41 della nostra Costituzione che descrive la "*possibile incidenza negativa delle attività economiche in senso ampio sulla realizzazione dei fini primari indicati dalla Costituzione*". Il riferimento, in particolare, è alla lesione della dignità umana. A. MORACE PINELLI, *Introduzione*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 1-22.

[96] E. S. DOVE, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in *Journal of Law, Medicine & Ethics*, 2018, 46(4), 1013-1030.

Il GDPR ha avuto un impatto significativo sulle pratiche di trattamento dei dati sia per le organizzazioni europee che per quelle che operano a livello internazionale. La sua attuazione ha richiesto investimenti in risorse umane, tecnologia e formazione. Tuttavia, ha anche contribuito a migliorare la consapevolezza sulla privacy dei dati e a rafforzare la fiducia degli individui nel controllo dei propri dati personali.

Sebbene la rete favorisca la piena espressione dei diritti della personalità, la diffusione e la naturale persistenza di dati personali inesatti, incompleti, o ormai non pertinenti rischiano di compromettere l'integrità dell'individuo. Questo fenomeno trasforma il tradizionale concetto statico di identità personale, introducendo una dimensione più fluida e dinamica[97]. Un esempio emblematico, (e collegabile al caso Warren e Brandeis descritto in precedenza) dell'effetto della rete e della necessaria regolazione degli effetti che questa produce sui diritti individuali è rappresentato dal diritto all'oblio, la cui concezione, con l'avvento di Internet e delle reti telematiche, si è necessariamente dovuta modificare poiché la permanenza delle informazioni online elimina la necessità di ripubblicazione: le informazioni rimangono disponibili nel web senza essere necessariamente rimosse. Questo mutamento ha ridimensionato il concetto di 'tempo' nell'oblio, spostando l'attenzione dalla ripubblicazione alla permanenza dell'informazione online, creando un continuum temporale.

Con la direttiva europea 95/46/CE e il successivo Regolamento Generale sulla Protezione dei Dati (GDPR), il diritto all'oblio si è ampliato includendo, fra gli altri, il diritto alla cancellazione, all'accesso e all'opposizione al trattamento dei dati. In particolare, il GDPR introduce l'obbligo per i titolari del trattamento di notificare ai terzi la richiesta di

[97] M. FARINA, *Il diritto all'oblio nella governance dell'identificazione*, in *Federalismi.it*, 2020, 18, 95-111.

cancellazione di dati personali, inclusi i link e le copie che sono presenti online.

Nel dettaglio, la sentenza della Corte di Giustizia Europea (caso *Google Spain*) delinea il diritto all'oblio nei confronti dei motori di ricerca, ritenuti come dei veri e propri titolari del trattamento. Questi possono quindi essere obbligati a rimuovere i collegamenti a informazioni che, sebbene pubblicate legittimamente da terzi, risultano non più pertinenti, inadeguate o eccessive rispetto al tempo trascorso e alle finalità originarie. Non si tratta di cancellare i dati alla fonte, ma di evitare che vengano indicizzati e resi accessibili tramite ricerca, configurando un diritto a "non essere trovati" più che un vero e proprio diritto alla cancellazione totale[98]. Il bene giuridico che si vuole tutelare in questo caso è quello dell'identità. Il dato personale è, in ultima analisi, inadeguato o non pertinente rispetto all'identità di un soggetto. Il motore di ricerca è, infatti, idoneo a generare una vera e propria immagine online[99].

Un'ulteriore innovazione è costituita dall'articolo 5 del GDPR che rappresenta la base su cui si fonda l'intera disciplina della protezione dei dati personali. Fin dalle sue prime righe, il legislatore europeo definisce i principi che devono orientare qualsiasi attività di trattamento, stabilendo un vero e proprio quadro etico-giuridico. Il testo introduce, in primo luogo, il principio di liceità, correttezza e trasparenza, secondo cui i dati devono essere trattati nel pieno rispetto della legge e in modo chiaro nei confronti dell'interessato. La trasparenza non si riduce a un mero adempimento formale: implica, piuttosto, la possibilità per ogni individuo di conoscere come e per quali scopi le proprie informazioni vengano utilizzate. Segue il principio di limitazione

[98] G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, 2014, 29-42.
[99] G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di G. RESTA e V. ZENO-ZENCOVICH, Roma, Roma Tre Press, 2015, pp. 29-42.

delle finalità, che vincola il trattamento dei dati a obiettivi determinati e legittimi. Ogni uso ulteriore deve essere compatibile con tali finalità, pena l'illiceità del trattamento stesso. Il Regolamento, tuttavia, consente eccezioni motivate, come nel caso di trattamenti per finalità di archiviazione nel pubblico interesse, ricerca scientifica o storica e fini statistici, a condizione che vengano adottate misure adeguate di tutela previste dall'articolo 89. Il secondo comma dell'articolo 5 del GDPR introduce uno dei concetti più innovativi dell'intera riforma: il principio di responsabilizzazione (o *accountability*). Secondo il Regolamento, infatti, il titolare del trattamento non solo deve garantire il rispetto dei principi generali del trattamento dei dati personali, ma deve essere anche in grado di dimostrare concretamente tale conformità.

Questa disposizione rappresenta un cambiamento di rilievo rispetto alla normativa precedente, poiché assegna ai titolari una responsabilità attiva nella definizione delle modalità, delle garanzie e dei limiti del trattamento, nel pieno rispetto delle disposizioni normative e dei criteri indicati dal Regolamento. Non si tratta più di un semplice rispetto passivo delle regole, ma di un approccio proattivo, che richiede di valutare e gestire i rischi legati al trattamento dei dati in maniera mirata e documentabile.

L'adozione di un approccio standardizzato e uguale per tutti i titolari, infatti, sarebbe risultata inefficace, rischiando di imporre strutture organizzative rigide e inadeguate rispetto alla realtà delle diverse organizzazioni. Al contrario, il principio di responsabilizzazione consente di adattare le misure di protezione dei dati alle specificità del contesto, promuovendo una gestione più efficace e consapevole delle informazioni personali, coerente con i rischi e le caratteristiche del trattamento effettuato.

Un altro elemento di equilibrio è rappresentato dal principio di limitazione della conservazione, che impone di non mantenere i dati più a lungo di quanto strettamente necessario. È ammessa una conservazione prolungata solo per scopi di ricerca o archiviazione, purché siano garantiti

elevati livelli di sicurezza e anonimato. Allo stesso modo, il principio di minimizzazione dei dati impone di raccogliere solo le informazioni realmente pertinenti rispetto agli scopi perseguiti, riducendo al minimo l'eccesso informativo e il rischio di trattamenti invasivi. Dal punto di vista qualitativo, il principio di esattezza obbliga i titolari del trattamento ad assicurare che i dati siano corretti e aggiornati, prevedendo la tempestiva rettifica o cancellazione di quelli inesatti o non più pertinenti. Infine, il principio di integrità e riservatezza sintetizza l'obiettivo di fondo del GDPR: garantire che i dati siano trattati in modo da assicurare un livello adeguato di sicurezza contro accessi non autorizzati, distruzioni o perdite accidentali, attraverso misure tecniche e organizzative proporzionate. Nel loro insieme, questi principi non rappresentano soltanto regole tecniche, ma delineano un modello di responsabilità e trasparenza che mira a bilanciare le esigenze dell'innovazione digitale con la tutela della persona e della sua dignità. A completamento di questo quadro, l'articolo 6 del GDPR definisce le condizioni di liceità del trattamento, confermando che ogni operazione sui dati deve poggiare su una base giuridica appropriata. In continuità con il Codice della privacy italiano (D.lgs. 196/2003), il Regolamento stabilisce che il trattamento è lecito se sussiste almeno una delle seguenti condizioni: il consenso dell'interessato; la necessità di eseguire un contratto o misure precontrattuali; l'adempimento di obblighi legali; la tutela di interessi vitali dell'interessato o di terzi; l'esecuzione di un compito di interesse pubblico o l'esercizio di pubblici poteri; o il perseguimento di un interesse legittimo del titolare, purché non prevalgano i diritti e le libertà fondamentali dell'interessato.

Sebbene queste basi giuridiche siano in linea con la disciplina nazionale precedente, il GDPR introduce significative innovazioni, rafforzando la protezione dei diritti degli interessati, chiarendo il ruolo del consenso e definendo più precisamente le responsabilità del titolare del trattamento. L'insieme dei principi generali e delle condizioni di liceità non

costituisce dunque solo un insieme di regole operative, ma rappresenta un vero e proprio modello di governance dei dati personali, fondato sul bilanciamento tra innovazione tecnologica, trasparenza e tutela della dignità della persona[100].

1.4 Il Data Governance Act

Il Data Governance Act (Regolamento UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 sulla governance dei dati europei che modifica il Regolamento (UE) 2018/1724) rappresenta un importante pilastro della Strategia Europea per i Dati. L'adozione del suddetto regolamento, intervenuta dopo l'introduzione di ben tre direttive: nel 2003[101], nel 2013[102] e, da ultimo nel 2019 con la Direttiva n. 1024 sul riutilizzo dei dati non sensibili e non soggetti a segreto industriale e commerciale, costituisce un ulteriore tassello nella definizione di un quadro regolativo integrato e uniforme per la gestione del mercato dei dati[103].

Questo regolamento segna il passaggio, desiderato dall'Unione Europea, dalla *data protection* alla *data governance*. Secondo la precisa diagonale di quest'ultima la necessità attuale è quella di definire il "costituzionalismo europeo" tramite l'applicazione di alcuni principi chiave, tra cui: il rispetto dei diritti fondamentali della persona e della concorrenza sana tra le imprese, con l'applicazione del cosiddetto principio *FAIR*, definito

[100] A. TORTORA, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del Data Protection Officer (DPO): incidenza sulla attività della pubblica amministrazione*, in *Amministrativ@mente – Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2018, 19-21.
[101] Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico, in *Gazzetta ufficiale dell'Unione europea*.
[102] Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013, che modifica la Direttiva 2003/98/CE, in *Gazzetta ufficiale dell'Unione europea*.
[103] C. SPINELLI, Il regolamento (UE) 2022/868 sulla governance dei dati e le sue possibili ricadute sulle misure di inclusione lavorativa delle persone con disabilità, in *Federalismi.it*, 2023, 9, 256-269.

nella direttiva Open Data come l'acronimo di 'dati' reperibili, accessibili, interoperabili, riutilizzabili. In questo contesto, la disciplina si presenta più di stampo promozionale che precettivo o sanzionatorio (a differenza di altri interventi). Essa non è quindi una normativa di divieto poiché l'obiettivo dell'Unione è piuttosto quello di sollecitare (non di vietare) offrendo delle opportunità al contrario di prospettare degli intenti sanzionatori. Si parla infatti di "facoltà" e non di obbligo di riutilizzo dei dati per gli enti pubblici[104].

Com'è stato per la proprietà, anche il diritto alla privacy, finanche nella sua accezione attuale, comprensiva del diritto alla protezione dei dati personali, si è necessariamente dovuto confrontare con il principio di solidarietà[105], il quale, allo stesso tempo rappresenta un "limite", nella prospettiva dell'inclusione e dell'apertura, e un "orizzonte", nella logica della condivisione. Si tratta di un confronto che va collocato in un più lungo percorso di maturazione, destinato a intraprendere la strada dell'utilizzabilità ulteriore dei dati, rispetto all'originaria finalità del trattamento (c.d. *secondary use*), per giungere, da ultimo, alla dimensione altruistica del trattamento, scolpita nel Data Governance Act[106].

---

[104] D. POLETTI, *Il quadro normativo del Data Governance Act: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 65-82.

[105] *"La Costituzione italiana, all'art. 2, pone l'enunciazione dei doveri inderogabili di solidarietà in parallelo al riconoscimento ed alla garanzia dei diritti inviolabili dell'uomo. Il principio di solidarietà trova, quindi, il proprio fondamento in tale disposizione, nella parte in cui, in perfetta simmetria con il riconoscimento dei diritti inviolabili dell'uomo, stabilisce che la Repubblica «richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale». Da una parte, «la Costituzione afferma il primato, l'indipendenza originaria della persona umana, cioè, la priorità di valore rispetto allo Stato come ad ogni altra autorità o struttura sociale dell'uomo, della sua inviolabile dignità che si esprime nei suoi diritti, assunti perciò come inviolabili, nella loro essenza, da ogni potere statale». Dall'altra, impone l'adempimento di doveri che, in forza dell'espressa connotazione solidaristica, rivolge al soddisfacimento di esigenze che fanno capo agli stessi membri della collettività che sono titolari dei diritti."* In: F. POLACCHINI, *Doveri costituzionali e principio di solidarietà*, Bologna, Bononia University Press, 2016.

[106] F. BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Il diritto dell'informazione e dell'informatica*, 2023, 3, 481-518.

Gli obiettivi fondamentali del regolamento in esame sono i seguenti: rendere disponibili i dati del settore pubblico per il riutilizzo; favorire la condivisione dei dati tra le imprese; consentire l'uso dei dati per scopi altruistici. Le imprese possono infatti condividere i propri dati insieme al relativo know-how, come competenze, esperienze e strumenti operativi (ad esempio software, algoritmi) andando a contribuire alla formazione di un processo definito come "*corporate philanthropy*"[107], che include anche la condivisione di risorse per condurre analisi e diffondere i risultati per un utilizzo più ampio (si pensi alla lotta al cambiamento climatico, alla ricerca scientifica, all'assistenza sanitaria o al miglioramento della mobilità pubblica). Ciò è rilevante soprattutto per soggetti che dispongono di grandi quantità di dati, ma non hanno il personale o la tecnologia per sfruttarli appieno. Tali dati verrebbero raccolti in un unico spazio europeo dei dati, a cui possano attingere, a parità di condizioni, tutti gli operatori economici, piccole imprese incluse. In questo modo si andrebbe a scardinare l'oligopolio delle principali *digital companies*[108].

Tuttavia, il concetto di 'donazione' di dati si scontra con il diritto alla protezione dei dati personali e, di conseguenza, la Commissione europea ha sostituito il termine donazione con 'altruismo', suscitando ugualmente delle perplessità, poiché ciò potrebbe implicare che il non condividere i dati venga considerata una manifestazione di 'egoismo'.

È' importante evidenziare che, nel regolamento in discussione, il servizio di intermediazione dei dati venga definito come un servizio finalizzato a creare rapporti commerciali per la condivisione dei dati tra un numero indefinito di interessati e titolari dei dati da un lato, e gli utenti dei

[107] M. STEMPECK, *Sharing data is a form of corporate philanthropy*, in *Harvard Business Review*, 24 luglio 2014, https://hbr.org/2014/07/sharing-data-is-a-form-of-corporate-philanthropy, consultato da ultimo il 14.10.2025.
[108] A. MORACE PINELLI, *Introduzione*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 1-22.

dati dall'altro. Questo servizio può essere realizzato attraverso strumenti tecnici, giuridici o di altro tipo, con l'obiettivo di facilitare anche l'esercizio dei diritti degli interessati nei confronti dei propri dati personali.

La condivisione dei dati d'altro canto è definita come la fornitura di dati da un interessato o titolare dei dati a un utente dei dati, sia per utilizzi congiunti che individuali, basata su accordi volontari o su disposizioni del diritto dell'Unione o nazionale, e può avvenire direttamente o tramite un intermediario, inclusi accordi di licenza aperta o commerciale, sia a titolo gratuito che dietro compenso.

Inoltre, l'altruismo dei dati è definito come la condivisione volontaria di dati, basata sul consenso degli interessati al trattamento dei dati personali, o su autorizzazioni di altri titolari dei dati, che consentono l'uso dei loro dati non personali. Questo avviene senza richiedere o ricevere un compenso superiore alla copertura dei costi per la messa a disposizione dei dati, perseguendo obiettivi di interesse generale stabiliti dal diritto nazionale, come l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, e la ricerca scientifica nell'interesse collettivo[109].

La base giuridica del DGA è costituita dall'art. 114 del TFUE. A tale proposito, la competenza concorrente del mercato consente agli Stati membri di adottare regole nazionali fino a quando uno specifico aspetto non sia pienamente regolamentato con atti di diritto derivato. Tuttavia, è importante ricordare che la competenza dell'Unione in materia di sviluppo tecnologico non impedisce agli Stati membri di continuare ad esercitare la loro competenza, come previsto dall'art. 4, par. 3, TFUE. La scelta dello strumento del regolamento è giustificata dalla necessità di garantire un'applicazione uniforme delle norme. Allo stesso tempo, il regolamento

[109] S. ORLANDO, *Il coordinamento tra la direttiva 2019/770 e il GDPR. L'interessato consumatore*, in. *Persona e Mercato*, 2023, 222-241.

lascia agli Stati membri un margine di discrezionalità per la definizione di alcuni aspetti riguardanti gli organismi competenti.

In ogni caso, il DGA va ad integrare il quadro normativo del GDPR che rimane il regolamento di riferimento per la protezione dei dati personali[110]. Le motivazioni economiche, infatti, non possono sbiadire quella che è la tutela della persona, la prevalenza del GDPR sul DGA in caso di conflitto è infatti stabilita dal legislatore europeo, ribadendo la centralità del rispetto dei diritti fondamentali.

Il Regolamento in esame si articola su quattro direttrici principali: il riutilizzo di dati specifici detenuti da soggetti pubblici (Capo II); l'intermediazione dei dati (Capo III); la disponibilità dei dati per fini altruistici (Capo IV); e, infine, l'istituzione di un nuovo sistema di governance dei dati e un regime sanzionatorio (Capo V e Capo VI). Dal quadro descritto emerge una nuova modalità di bilanciamento tra il valore economico dei dati e la loro libera circolazione. Tale approccio si concretizza nell'abbandono del principio di *jus excludendi alios* – tipico della protezione dei dati personali – e nell'adozione di una logica di inclusione, propria della solidarietà. Questa evoluzione riflette una diversa interpretazione del principio solidaristico, promuovendo un modello in cui la condivisione dei dati non riguarda solo l'utilità economica, ma diventa anche un imperativo etico e sociale, finalizzato al bene comune e all'innovazione collettiva[111].

L'articolo 10 del Data Governance Act (DGA) definisce tre principali categorie di servizi di intermediazione dei dati, tutti soggetti a una procedura di notifica obbligatoria. La prima categoria riguarda i servizi finalizzati alla condivisione dei dati tra attori di mercato, ovvero tra titolari dei dati e

[110] F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Annali AISDUE*, 3, 2021, 58-75.
[111] M. AMENDOLA, *Il principio solidaristico e il Data Governance Act*, Università di Salerno, 2023.

potenziali utenti, inclusi i mezzi tecnici o strumenti necessari per facilitare tale intermediazione.

La seconda tipologia di servizi riguarda l'intermediazione tra gli interessati che intendono rendere disponibili i propri dati personali o i dati non personali, e i potenziali utenti dei dati. Questi servizi devono, in particolare, consentire l'esercizio dei diritti degli interessati come previsto dal GDPR, garantendo trasparenza e controllo sulle informazioni condivise.

Infine, il DGA riconosce una terza categoria denominata "cooperative di dati". Tali cooperative sono organizzazioni costituite da interessati, piccole e medie imprese o singoli membri, che hanno l'obiettivo principale di assistere i propri membri nell'esercizio dei loro diritti sui dati. Le cooperative offrono supporto nella valutazione delle condizioni di trattamento dei dati, nello scambio di opinioni riguardo alle finalità e alle modalità del trattamento e nella negoziazione dei termini di utilizzo dei dati per conto dei membri, prima che questi concedano il proprio consenso o autorizzino il trattamento di dati personali o non personali.

Queste disposizioni sottolineano come il DGA miri a creare un ecosistema regolamentato per la circolazione dei dati, garantendo protezione degli interessati e promuovendo pratiche trasparenti e responsabili nell'intermediazione dei dati, rafforzando così il diritto alla gestione consapevole delle informazioni personali[112].

È importante precisare che il Regolamento stabilisce una serie di regole comuni da applicare nel caso in cui l'ente pubblico decida, eventualmente dietro compenso, di permetterne l'uso. Inoltre, l'ente pubblico può fornire "servizi di intermediazione dei dati" e assumere il ruolo di "titolare dei dati" ai sensi del Regolamento. Agli enti pubblici spetta il

[112] M. TAMPIERI, *Cooperative di dati per la tutela della salute*, in *EU Data Cooperatives: L'ingresso delle cooperative di dati nell'ordinamento europeo*, a cura di F. BRAVO, Torino, Giappichelli, 2024, 434-442.

compito di garantire l'accesso legittimo ai dati per il loro riutilizzo, mentre accordi di esclusiva sul riutilizzo dei dati sono vietati[113].

In questo contesto, l'interessato può richiedere che i propri dati, siano essi personali o non personali, vengano messi a disposizione di un "utente dei dati", il quale può utilizzarli per scopi commerciali o non commerciali. La regolazione europea recente è orientata a rendere disponibili grandi quantità di dati a vantaggio del mercato, promuovendo la circolazione e condivisione degli stessi nel rispetto dei diritti degli interessati e dei terzi coinvolti. Con maggiore cautela rispetto al settore pubblico, anche il settore privato è incluso in questo quadro normativo favorevole alla condivisione e accesso ai dati. In particolare, l'Unione Europea ha adottato norme che incentivano soprattutto la condivisione volontaria dei dati, mentre solo in rari e specifici casi sono previste misure obbligatorie di accesso ai dati da parte di soggetti pubblici o terzi del mercato[114]. Il DGA prevede inoltre che ciascuno stato membra debba designare sia uno o più organismi o enti pubblici competenti per settore ad assistere gli enti pubblici nelle attività di gestione delle richieste di accesso alle categorie di dati, ma anche le autorità competenti a registrare le organizzazione che svolgono compiti di *data altruism* e quelle che sono competenti alla ricezione di notifiche dai fornitori di servizi di *data sharing*[115].

È ormai un dato di fatto che dall'analisi, strutturazione o destrutturazione di dati personali, in particolare delle cosiddette "categorie particolari di dati" (come definite dall'art. 9 del GDPR), sia possibile estrarre numerose informazioni. Questa pratica comporta vantaggi indiscutibili, sia in termini di potere e controllo che sotto il profilo economico. Si pensi, ad

---

[113] G. CERRINA FERONI, *Governare la rete per governare i diritti: quale cornice strutturale per il Data Governance Act?*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 23-32.
[114] E. CREMONA, *Quando i dati diventano beni comuni: Modelli di data sharing e prospettive di riuso*, in *Rivista Italiana di Informatica e Diritto*, 2024, 5(2), 111-130.
[115] Articolo 7, 13 e 23 del Regolamento (UE) 2022/868.

esempio, alla business intelligence, al *FinTech*, oppure all'impatto socioeconomico e politico legato alla disponibilità, utilizzo e riutilizzo di dati pandemici, anche di natura transfrontaliera, relativi a un determinato Stato o continente. Dall'analisi di questi dati possono derivare benefici che si riflettono sia a livello economico che politico[116]. L'idea che l'informazione accessibile senza restrizioni possa costituire un "bene competitivo" e strategico in ambito economico è sostenuta dall'interesse sempre maggiore di numerose aziende specializzate che offrono piattaforme digitali open source, le quali centralizzano la raccolta e l'armonizzazione dei big data. Tali dati, provenienti da pubbliche amministrazioni ed enti privati, vengono resi disponibili per il riutilizzo da parte di cittadini e di altre entità giuridiche, semplificando così l'accesso e la fruizione delle informazioni[117].

In questa ottica, è significativo notare come il Data Governance Act offra una definizione autonoma di 'dato', segnando una discontinuità rispetto al contesto legislativo europeo, che ha tradizionalmente formulato tale definizione in modo negativo e in opposizione ai 'dati personali'[118]. Come sottolineato da L. Petrone, per 'dati' si intendevano prima quelli diversi dai dati personali definiti dall'art. 4, punto 1, del Regolamento (UE) 2016/679. Infatti, nel diritto dell'Unione non vi era, sino all'entrata in vigore del Regolamento UE 2022/868, una definizione normativa di 'dato'. L'unica definizione che era possibile ritrovare nel panorama legislativo era quella di 'dati personali', definita sin dalla Direttiva 1995/46/CE (art. 2, comma 1, lett. A) e poi dall'art. 4, n. 1, Regolamento (UE) 2016/679 come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che può essere*

[116] C. IURILLI, *La tutela del dato personale alla prova del Data Governance Act. Data sharing, reclamo e tutela giurisdizionale effettiva*, in *Judicium*, 3, Pacini Giuridica, 2024.
[117] G. CRUPI, *Considerazioni preliminari sul riuso delle risorse digitali*, in *DigItalia*, 18(2), 2023, 15-23.
[118] L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 39(3), 2023, 800-817.

identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Conseguentemente, come afferma l'autore, per 'dato', potevano essere intesi tutti quegli elementi che non sono direttamente riconducibili alla definizione sopra riportata. L'articolo 2 del DGA, paragrafo 1, introduce una nuova definizione e stabilisce chiaramente che per 'dato' si debba intendere "(…) *qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva*". Nonostante ciò, il Data Governance Act mantiene un costante richiamo alla necessità del consenso per il trattamento dei dati personali, come previsto dal GDPR, anche se questo si rivela spesso un mezzo di protezione insufficiente. È interessante notare che il Regolamento (UE) 2016/679 (GDPR) si fonda su un modello di consenso che, in ultima analisi, potrebbe essere descritto come un "vaso di cristallo fragile e dal contenuto eterodeterminato"[119]. Infatti, i contenuti delle policy che regolano il trattamento dei dati risultano spesso così complessi e poco comprensibili da generare un disinteresse generale alla loro consultazione da parte della maggior parte degli interessati. L'incertezza, del resto, rappresenta un elemento chiave dell'asimmetria informativa, accentuata dall'evoluzione tecnologica e dai processi di raccolta dati. Il progresso tecnologico ha reso la raccolta e l'utilizzo delle informazioni personali spesso impercettibili per l'utente, che raramente ha piena consapevolezza della quantità e della tipologia di dati acquisiti, nonché delle modalità di impiego e delle relative conseguenze. In tale contesto, l'assenza

[119] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 47 ss.
S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Tecnologie e diritti*, Bologna, Il Mulino, 1995, 79-80.

di consapevolezza circa i limiti della propria conoscenza porta le persone a sperimentare un certo grado di incertezza riguardo ai dati da condividere[120].

L'applicazione del DGA solleva inoltre alcune problematiche rilevanti riguardo alla protezione dei dati personali e alla sua compatibilità con il GDPR. Tre punti in particolare meritano attenzione.

In primo luogo, vi è una possibile discrepanza con i principi fondamentali del GDPR. L'articolo 5 del regolamento europeo stabilisce infatti che i dati personali devono essere raccolti esclusivamente per finalità specifiche, esplicite e legittime, e non ulteriormente trattati in modi incompatibili con tali scopi. Sebbene il regolamento preveda eccezioni per l'archiviazione di dati a fini di interesse pubblico, ricerca scientifica o statistiche, l'obiettivo del DGA di favorire il riutilizzo dei dati del settore pubblico solleva interrogativi sul rischio che informazioni personali possano essere impiegate in modi inaspettati o potenzialmente dannosi per gli interessati.

Il secondo punto riguarda la sicurezza dei dati anonimizzati. Il GDPR non si applica ai dati pienamente anonimi; pertanto, il DGA fa affidamento su una corretta anonimizzazione dei dati per rispettare i limiti di finalità. Tuttavia, è noto che esistono algoritmi avanzati per la de-anonimizzazione e la re-identificazione dei soggetti, e l'efficacia di tali tecniche è destinata a crescere con i progressi in machine learning e intelligenza artificiale. Ne consegue che la capacità dei metodi di protezione della privacy indicati nel DGA di prevenire il rischio di re-identificazione rimane incerta, con preoccupazioni analoghe anche per i dati non personali soggetti a riservatezza commerciale.

[120] J. ARPETTI, *Economia della privacy: una rassegna della letteratura*, in *Media Laws*, 2018, 2, 267-297.

Infine, vi è una questione relativa alle autorità nazionali per la protezione dei dati, il cui carico di lavoro sembra aumentare notevolmente con il DGA. Ad esempio, il considerando 15 del DGA prevede che prima di concedere l'accesso ai dati per il riutilizzo, gli enti pubblici debbano effettuare valutazioni di impatto sulla protezione dei dati e consultare le autorità competenti, conformemente agli articoli 35 e 36 del GDPR. Queste consultazioni comprendono anche aspetti legati all'anonimizzazione. Tuttavia, secondo il considerando 26, i nuovi organismi di monitoraggio dei servizi di intermediazione e delle organizzazioni di "*data altruism*" non dispongono di funzioni di vigilanza stringenti, riservate invece alle autorità di protezione dei dati[121].

1.5 Il Data Act

Il 22 dicembre 2023 è stato pubblicato nella Gazzetta ufficiale dell'Unione europea il Regolamento (UE) 2023/2854, relativo a norme armonizzate sull'equità dell'accesso e dell'uso dei dati, noto come Regolamento sui dati o Data Act. Questo nuovo quadro normativo modifica il Regolamento (UE) 2017/2394 del Parlamento europeo e del Consiglio, del 12 dicembre 2017, sulla cooperazione tra le autorità nazionali competenti per l'applicazione della normativa in materia di protezione dei consumatori, e la Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative per la tutela degli interessi collettivi dei consumatori. Sebbene il nuovo regolamento sia entrato in vigore l'11 gennaio 2024, è applicabile in tutti gli Stati membri solo a partire dal 12 settembre 2025[122].

[121] J. RUOHONEN, S. MICKELSSON, *Reflections on the Data Governance Act*, in *Digital Society*, 2(1), 2023, 10.
[122] É. RANÇON, *Publication du Data Act: Observations sous règlement (UE) 2023/2854 du Parlement et du Conseil du 13 décembre 2023*, in *Dalloz IP/IT*, 2024, 5.

Il Data Act rappresenta un importante indicatore della crescente consapevolezza dell'Unione Europea riguardo alle lacune nel proprio sistema normativo e ai cambiamenti che investiranno il diritto europeo dei dati nei prossimi anni. In questo contesto, il Data Act e il Data Governance Act, anch'esso recentemente approvato, si configurano come due strumenti normativi interconnessi, miranti a stabilire un nuovo modello di governance dei dati a livello europeo.

Il Data Governance Act si occupa di disegnare una cornice circolatoria, ricoprendo una funzione promozionale, alla quale il Data Act fornisce concreta attuazione. Ciò è posto con la volontà di utilizzare dati interoperabili e di elevata qualità provenienti da diversi settori, poiché questi "*aumentano la competitività e l'innovazione e garantiscono una crescita economica sostenibile. Gli stessi dati possono essere utilizzati e riutilizzati per una varietà di scopi e in misura illimitata, senza alcuna perdita in termini di qualità o quantità*[123]".

Le norme contenute nel testo del Data Act necessitano, come d'altronde quelle di molti altri regolamenti recenti dell'unione, dell'intervento interpretativo dei tecno-giuristi per mediare tra sfera giuridica e sfera tecnologica. Tale dimensione alternativa è rappresentata infatti da un linguaggio utilizzato nei vari regolamenti decisamente complesso e ricco di tecnicismi che fanno emergere l'importanza del ruolo dell'interprete. L'oggetto del regolamento, come si desume dall'art.1 è infatti legato ai dati generati da un prodotto connesso e da un servizio correlato. Nel contesto del regolamento l'ago della bilancia si sposta dal profilo della protezione dati a quello della circolazione e valorizzazione degli stessi[124]. Per promuovere un mercato europeo dei dati equo ed efficiente, capace di generare valore,

[123] Considerando 1 del Data Act.
[124] C. CARICATO, *Commento articolo 1*, in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 269-300.

stimolare l'innovazione e ridurre le situazioni di dominio informativo, l'Unione Europea ha scelto di non adottare un modello fondato sulla proprietà dei dati. Questa scelta rappresenta un punto di svolta significativo, soprattutto se si considera che nelle fasi iniziali del dibattito vi erano pressioni in senso opposto, orientate verso il riconoscimento di diritti di proprietà, anche di natura intellettuale, sui dati stessi.

Tale impostazione, tuttavia, è stata espressamente esclusa nell'elaborazione della normativa europea in materia di dati. Ciò risulta evidente, ad esempio, nell'articolo 43 del Data Act, che disciplina i dati generati dall'Internet of Things (IoT), e nel considerando 5 del medesimo atto, dove vengono delineati gli obiettivi generali del regolamento. Entrambi i riferimenti confermano la volontà del legislatore di non trasformare i dati in oggetti di proprietà esclusiva, ma di favorirne un uso condiviso e regolato[125].

Il paragrafo d'apertura del regolamento si concentra quasi interamente sulla condivisione dei dati, includendo la messa a disposizione dei dati del prodotto connesso e di un servizio correlato all'utente del prodotto o servizio, la messa a disposizione di dati da parte dei titolari ai destinatari dei dati, e la messa a disposizione di dati da parte dei titolari agli enti pubblici, alla Commissione, alla Banca Centrale Europea e ad altri organismi dell'Unione, in presenza di necessità eccezionali per l'esecuzione di compiti specifici svolti nell'interesse pubblico.

Dal quadro delineato emergono tre distinti canali di circolazione dei dati (personali e non personali):

- In primo luogo i dati che vengono messi a disposizione all'utente di un prodotto connesso o di un servizio correlato da parte del titolare dei dati, quest'ultimo inteso come da art. 2 paragrafo 13 del Data Act: "*una persona fisica o giuridica che ha il diritto o l'obbligo,*

[125] T. MARGONI, C. DUCUING, L. SCHIRRU, *Data Property, Data Governance and Common European Data Spaces*, in *Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht*, 2023.

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";

- In secondo luogo i dati che, da parte del titolare dei dati, vengono messi a disposizione ai destinatari dei dati, da intendersi, secondo l'art. 2 paragrafo 14, come: "*una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione*;"
- Infine, l'ultimo canale di circolazione dei dati che può considerarsi all'interno del fenomeno descritto come "altruismo dei dati" contiene i dati messi a disposizione dal titolare dei dati ad enti pubblici se in presenza di necessità eccezionali o per finalità di pubblico interesse, come descrive l'art. 2 al paragrafo 29: "*una situazione eccezionale, limitata nel tempo, come un'emergenza di sanità pubblica, un'emergenza derivante da calamità naturali, una grave catastrofe di origine antropica, compreso un grave incidente di cibersicurezza, che incide negativamente sulla popolazione dell'Unione o su tutto o parte di uno Stato membro, con il rischio di ripercussioni gravi e durature sulle condizioni di vita o sulla stabilità economica, sulla stabilità finanziaria, o di un sostanziale e immediato degrado delle risorse economiche nell'Unione o nello Stato membro o negli Stati membri*

interessati e che è determinata o dichiarata ufficialmente in conformità delle pertinenti procedure previste dal diritto dell'Unione o nazionale".

Alla luce delle più recenti evoluzioni tecnologiche e in un mondo iperconnesso, il Data Act si concentra in particolare sugli oggetti e servizi connessi alla rete internet (*l'Internet of things* – IoT) senza tralasciare i servizi di cloud computing. Poiché il mercato è dominato da attori che esercitano una forte presenza commerciale e dispongono di un maggiore potere contrattuale, questa normativa dovrebbe contribuire a ripristinare un equilibrio competitivo tra i vari attori, senza trascurare le questioni relative alla proprietà intellettuale e al segreto commerciale.

Il nuovo regolamento mira a colmare quel vuoto giuridico lasciato dai regolamenti precedentemente adottati, cercando innanzitutto di affrontare le problematiche giuridiche contemporanee legate all'utilizzo dei dati per consentire la creazione di servizi accessori o per ottimizzare i servizi pubblici, affrontando anche la questione del potenziale industriale ed economico associato ai dati in relazione ai vari attori coinvolti, siano essi imprese private, enti del settore pubblico o consumatori di tali prodotti e servizi[126]. Come nel Data Governance act, nel Data Act vengono inserite nuove definizioni tra cui spiccano, in primo luogo, quelle all'art. 2 di "prodotto connesso": "*un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente*;" e di "servizio correlato": "*un servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto al*

[126] C. SAILLANT, *Stratégie européenne pour les données : adoption du Data Act par le Conseil de l'Union européenne*, in *Dalloz actualité*, 2023.

momento dell'acquisto, della locazione o del noleggio in modo tale che la sua assenza impedirebbe al prodotto connesso di svolgere una o più delle sue funzioni o che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto connesso." Risulta utile precisare che, a partire dal considerando 17 del Data Act, la maggior parte dei servizi digitali rientrerebbe nella categoria dei servizi correlati, ciononostante, alcuni servizi digitali come, ad esempio, la connettività (intesa come la capacità che sistemi diversi hanno di collegarsi e comunicare fra loro al fine di scambiarsi informazioni), l'alimentazione e alcuni servizi post-vendita non sono da intendersi come servizi correlati. Questo perché, al fine di offrire un servizio correlato, il provider dovrà prima aver ricevuto i dati del prodotto e, solo una volta instauratosi un rapporto di natura contrattuale fra utente e fornitore (rendendo un servizio correlato produttivo di dati), quest'ultimo diventerà titolare di dati[127].

Questo modello ha come obiettivo principale quello di contrastare l'accumulo esponenziale di potere nelle mani di soggetti, pubblici e privati, al di fuori dell'Unione. Inoltre, si propone di tutelare la sovranità degli Stati membri, contribuendo alla riduzione della quantità di dati che lasciano il territorio europeo. Ciò è fondamentale per evitare che tali dati diventino una risorsa preziosa per autorità o industrie situate al di fuori dell'Unione[128]. Questi atti normativi, insieme al Digital Markets Act, mirano a ridefinire le condizioni di concorrenza nel mercato digitale, facilitando la crescita di nuovi modelli di business basati sulla cooperazione, grazie a una maggiore accessibilità ai dati.

Secondo il GDPR, il trasferimento dei dati dovrebbe avvenire nel modo più rapido e diretto possibile, consentendo all'interessato di richiedere

---

[127] C. CARICATO, *Commento articolo 1*, in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 269-300.

[128] S. TORREGIANI, *Il Data Act: una versione europea del Data Nationalism?*, in *Rivista italiana di informatica e diritto*, 5(2), 2023, 131-146.

al titolare del trattamento di inviare i propri dati a un terzo titolare (o a un altro "utente dei dati", come definito nel Data Governance Act). Tuttavia, nella pratica, molte grandi piattaforme rendono complicato l'esercizio del diritto alla portabilità. Questo diritto, dal punto di vista tecnologico, presuppone che i dati siano forniti attraverso una procedura che non sia eccessivamente complessa e in un formato interoperabile[129]. Le nozioni richiamate trovano definizione all'art 2 e precisamente al paragrafo n. 15 in cui i "dati del prodotto" sono definiti come: "*dati generati dall'uso di un prodotto connesso e progettati dal fabbricante in modo tale che un utente, un titolare dei dati o un terzo, compreso se del caso il fabbricante, possano reperirli tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo*;" e i "dati di un servizio correlato", definiti al paragrafo 16 come: "*dati che rappresentano la digitalizzazione delle azioni o degli eventi degli utenti relativi al prodotto connesso, registrati intenzionalmente dall'utente o generati come sottoprodotto dell'azione dell'utente durante la fornitura di un servizio correlato da parte del fornitore*".

Il regolamento, nella sua definizione dei servizi di trattamento dei dati, stabilisce fin dall'inizio la volontà di consentire all'utente la possibilità cambiare il fornitore di trattamento con facilità. Questo cambiamento può avvenire in circostanze diverse e, per esempio, può riguardare lo stesso tipo di servizi, servizi differenti, oppure il trasferimento dei dati su un'infrastruttura di tecnologie dell'informazione e della comunicazione (ITC) locale.

Le istituzioni europee hanno espresso il desiderio che il trasferimento dei dati e degli asset digitali da un fornitore all'altro avvenga nelle migliori condizioni possibili, assicurando la cooperazione di tutte le parti coinvolte. A

[129] M. FEDERICO, B. PARENZO, *Le cooperative di dati tra persona e mercato: casi di studio*, in *De Iustitia*, 4, 2024, 1-12.

tale scopo, i diversi attori, siano essi il fornitore originario, quello di destinazione o il cliente stesso, sono tenuti a rispettare un obbligo di buona fede durante l'intero processo. Questo obbligo di buona fede implica la loro cooperazione per garantire che il cambiamento sia effettivo, che il trasferimento dei dati avvenga in modo tempestivo e che la continuità del servizio venga mantenuta.

In particolare, tali obblighi gravano principalmente sul fornitore originario, ma, per estensione, si applicano a qualsiasi fornitore che stipuli un contratto con un cliente. La finalità è quella di assicurare che il processo di transizione avvenga senza interruzioni o complicazioni, con un'attenzione particolare al rispetto delle tempistiche e alla protezione dei dati trasferiti[130].

Il Data Act si configura inoltre come il testo normativo più avanzato in materia di accesso e condivisione dei dati. Questo Regolamento si propone diverse finalità, tutte orientate a rimuovere al massimo gli ostacoli che attualmente limitano l'accesso e la condivisione dei dati tra consumatori e imprese, tra le imprese stesse e, in determinate condizioni, tra il settore pubblico e il mondo imprenditoriale. Una delle principali innovazioni del Regolamento è la garanzia che gli utenti di prodotti o servizi connessi, comunemente noti come "Internet of Things" (IoT), possano accedere in modo tempestivo ai dati generati dall'uso di tali dispositivi o servizi. Inoltre, il Regolamento riconosce agli utenti il "diritto" (art. 5) di condividere questi dati con terzi di loro scelta, imponendo così un obbligo ai titolari dei dati di rendere tali informazioni disponibili[131].

L'Autorità Garante francese (CNIL) si è pronunciata in materia nel documento: "*Stratégie européenne pour la donnée: la CNIL et ses*

[130] F. NAFTALSKI e M. KERAMBRUN, *L'impact du « Data Act » sur les obligations des fournisseurs de services de traitement de données, en particulier sur les prestataires de services de cloud computing*, in *Dalloz IP/IT*, 2024, 211.
[131] E. CREMONA, *Quando i dati diventano beni comuni: Modelli di data sharing e prospettive di riuso*, in *Rivista Italiana di Informatica e Diritto*, 2024, 5(2), 111-130.

homologues se prononcent sur le Data Governance Act et le Data Act"[132] andando ad individuare gli obiettivi primari che il Data Act propone di perseguire, ovvero:

- Facilitare la condivisione dei dati tra aziende (B2B) e con i consumatori (B2C), stabilendo in particolare un obbligo di rendere accessibili i dati generati dall'uso di oggetti connessi e servizi correlati, in cambio di una compensazione giusta ed equa;
- Consentire l'utilizzo dei dati detenuti dalle imprese e, a condizione di giustificare un bisogno eccezionale, da parte degli enti pubblici degli Stati membri e delle istituzioni, agenzie o organi dell'Unione;
- Facilitare il cambio di fornitore di servizi di elaborazione dei dati (cloud e edge computing) regolamentando le relazioni contrattuali tra fornitori di servizi e consumatori, e in particolare attraverso l'abolizione graduale delle spese di cambio per i consumatori;
- Prevedere l'elaborazione di norme di interoperabilità per i dati e il loro riutilizzo tra i vari settori;
- Mettere in atto garanzie contro l'accesso illecito da parte dei governi di paesi terzi ai dati non personali contenuti nel cloud.

In concreto, il Data Act è un regolamento il cui scopo è garantire equità all'interno dell'ambiente digitale, stimolando un mercato dei dati che sia sempre più competitivo, andando a creare delle occasioni di sviluppo per la *data based innovation* e rendendo i dati più accessibili a tutti. Si parla, come indicato, soprattutto di dati industriali, generati da Industrial IoT (Internet of Medical Things – IoMT, Smart Buildings, Smart Grids, smart Cities…) Secondo la Commissione, questi ultimi, all'80% non vengono utilizzati, e l'obiettivo del regolamento è quello di rendere l'Europa leader nell'economia

[132] CNIL, *Stratégie européenne pour la donnée : la CNIL et ses homologues se prononcent sur le Data Governance Act et le Data Act*, https://www.cnil.fr/sites/default/files/atoms/files/lettre_information_cnil_juillet_2022.html, consultato da ultimo il 15.10.2025.

dei dati andando a sfruttare le potenzialità sempre più crescenti dei dati industriali elencati. Si sottolinea che i sistemi IoT, per la loro peculiare natura a cavallo tra il mondo digitale e quello fisico, non elaborano solamente i dati, ma li generano[133].

Tuttavia, è necessario muovere delle osservazioni critiche al testo, poiché in esso rientrano anche i dati personali che derivano da oggetti connessi alla rete, come per esempio i dispositivi medici che, si ricorda, vengono generati da persone fisiche. Questi dispositivi permettono di raccogliere input biometrici, tra cui frequenza cardiaca, *sleep patterns*, informazioni relative alla fertilità. Si nota, dunque, che non si tratta di semplici scambi Business to Business o Business to Government, ma di scambi da Citizen to Business o Citizen to Government. A tal proposito il *Parere congiunto EDPB-GEPD 2/2022 sulla proposta del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati),* ha posto delle critiche al Data Act, poiché quest'ultimo potrebbe finire col normalizzare alcune pratiche di *datification* delle persone in Europa. Come forma di tutela dei diritti fondamentali è necessario domandarsi quali siano i limiti della riduzione in dati della persona umana (*data perimeter*) e quale sia la portata tollerabile della datificazione. In questo scenario gli interessati sono facilmente vittime di fatica del consenso (*consent fatigue*) per cui le continue richiesti di consenso possono portare alla cessione dei propri dati personali a diversi intermediari o *data recipients* che potranno usufruire o comunicare i dati anche a parti terze, per tipologie di finalità indeterminate.

Per questo motivo, la recente normativa sui dati potrebbe non offrire le tutele attese su dati sensibili, come quelli relativi alla salute e ai dati

[133]P. POLETTI, *Riforma dello spazio digitale europeo: DGA, proposta di Data Act e sicurezza delle informazioni*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 107-116.

biometrici[134]. Il Data Act limita solo in parte la possibilità di profilazione da parte di terzi: l'articolo 6(2)(b) vieta infatti l'uso dei dati ricevuti per fini di profilazione, "a meno che ciò non sia necessario per fornire il servizio richiesto dall'utente".

Detto ciò, è evidente che i redattori del Data Act erano ben consapevoli della natura funzionale della definizione di dato personale, tanto da includere tra i dati regolati sia quelli personali sia quelli non personali. Anche se la fonte dei dati non contiene informazioni personali identificabili, è probabile che includa comunque informazioni relazionali molto dettagliate. Inoltre, l'utente dei dati o terze parti potrebbero avere accesso ad ulteriori informazioni personali identificabili. In altre parole, le finalità previste e successive del trattamento tenderanno verosimilmente a comportare una combinazione di dati sia non identificabili personalmente sia identificabili personalmente[135].

1.6 Intelligenza artificiale tra trattamento di dati personali e governance nell'AI Act

1.6.1 Intelligenza artificiale e dati personali

L'intelligenza umana può essere definita, in termini semplici, come la capacità di apprendere e di applicare tecniche adeguate alla soluzione di problemi in un mondo incerto e in continua trasformazione. In concreto, il *problem-solving* richiede un insieme articolato di abilità (dalla comprensione linguistica all'apprendimento, dal pensiero astratto al ragionamento, fino alla capacità di pianificazione) la cui combinazione consente di rappresentare la conoscenza, per poi individuare e interpretare soluzioni. L'intelligenza

[134] M. GUGLIELMETTI, *Monetizzazione dei dati personali: breve analisi fondata sul valore della dignità umana e sulle «condizioni di mercato» della c.d. economia dei dati personali*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024, 33-53.
[135] S. STALLA-BOURDILLON, *Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU?*, in *European Journal of Risk Regulation*, 2025.

artificiale ha acquisito negli ultimi anni una crescente rilevanza grazie allo sviluppo di tecnologie in grado di emulare, almeno in parte, tali capacità umane nella risoluzione di problemi complessi. Alcuni esempi includono le applicazioni che permettono la generazione di immagini a partire da descrizioni testuali o la produzione di testi articolati su una vasta gamma di argomenti[136]. L'Intelligenza Artificiale, secondo il dizionario Oxford, è definita come la teoria e lo sviluppo di sistemi informatici in grado di svolgere compiti che un tempo richiedevano l'intelligenza umana, come il riconoscimento visivo, la comprensione vocale, il processo decisionale e la traduzione linguistica.

Il processo di regolamentazione dell'intelligenza artificiale all'interno dell'Unione Europea, che non è sfuggito ad un ampio dibattito, può essere visto come l'inizio di una trasformazione epocale, simile ad una "rivoluzione copernicana", che trova il suo compimento nell'adozione di un regolamento che si occupa di stabilire regole armonizzate per l'IA, il cosiddetto Artificial Intelligence Act (AI Act), che, pur rappresentando solo il primo passo, dà concreta attuazione a questa trasformazione, restando tuttavia ancora lontano da un completamento totale. Nell'AI Act si specifica che un sistema di IA è un software sviluppato con approcci e tecniche particolari, capace di generare output come contenuti, previsioni, raccomandazioni o decisioni, che a loro volta influenzano l'ambiente in cui interagiscono.

Da diversi anni la transizione digitale è considerata una delle priorità indiscusse dell'Unione Europea e, recentemente, tale priorità è diventata ancora più evidente, tanto nelle dichiarazioni ufficiali delle istituzioni europee quanto nella produzione di normative a livello sovranazionale.

Dal punto di vista istituzionale, la regolamentazione dell'IA è stata sollecitata da più fronti, con richieste che sono arrivate da tutte le principali

[136] F. BERTINI, *Artificial Intelligence and data privacy*, in *Sistemi intelligenti*, 2023, 35(2), 477-484.

entità che compongono l'ordinamento giuridico dell'Unione Europea, in un processo in cui si è sottolineato il ruolo attivo e propulsivo svolto dal Parlamento Europeo, così come il supporto e la spinta forniti dalla Commissione europea, senza dimenticare gli interventi e le prese di posizione del Consiglio europeo e del Consiglio dell'Unione Europea, che hanno contribuito, seppur in modo diverso, alla formulazione delle linee guida su questo tema[137].

Negli ultimi anni, come ampiamente discusso, il diritto del digitale ha visto un notevole incremento delle sue fonti normative a livello europeo. Il Regolamento Generale sulla Protezione dei Dati (GDPR) ha segnato profondamente lo scorso decennio, mentre l'inizio degli anni 2020 è stato caratterizzato da un aumento significativo delle normative comunitarie, tra cui il più atteso è stato il Regolamento sull'Intelligenza Artificiale (AI Act).

Questa forte aspettativa è giustificata sia da ragioni giuridiche che politiche. Infatti, l'Unione Europea è riuscita a creare, con il GDPR, un testo che è diventato un punto di riferimento non solo a livello europeo, ma anche a livello mondiale (grazie alla sua extra-territorialità.) L'AI Act si connota dell'ambizione di perseguire le stesse orme e di avere un impatto anche all'esterno dell'Unione (si pensi al "*Brussels effect*" generato dal GDPR). Tuttavia, questo nuovo regolamento deve inserirsi in un contesto normativo già ampio e complesso, il che porta inevitabilmente a contraddizioni, sia in termini di obiettivi sociali che di norme giuridiche[138]. La condivisione e la libera circolazione dei dati, il loro riutilizzo e l'altruismo dei dati (disciplinato dal DGA) si sviluppano lungo direttrici in parte divergenti, ma destinate a convergere nella necessaria integrazione con le istanze di protezione dei dati

[137] F. FERRI, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in *Quaderni AISDUE*, 2024, 2, 1-20.
[138] M. MORITZ, *Protection des données à caractère personnel et déploiement des IA: une conciliation impossible ? Le cas des décisions individuelles automatisées*, in *Dalloz IP/IT*, 2024, 506.

personali. In tale contesto, l'impiego di strumenti avanzati per la raccolta di dati e informazioni rende indispensabile un bilanciamento accurato tra interessi pubblici e diritti individuali. Questo bilanciamento si articola attorno a temi la cui rilevanza è fondamentale, quali la specificità del consenso, la trasparenza algoritmica, la responsabilità (accountability), la tutela della privacy, la sicurezza informatica e la protezione della proprietà intellettuale. L'attuale impianto regolatorio avverte con urgenza la necessità di armonizzare le spinte della trasformazione digitale (alimentata da big data, analisi dei dati e machine learning) con le garanzie offerte alla persona fisica, che deve poter esercitare il proprio diritto alla protezione dei dati personali in ogni momento[139].

Il regolamento stabilisce obblighi per i sistemi di intelligenza artificiale in base ai loro potenziali rischi e al loro livello di impatto, differenziando perciò i modelli di IA "a uso generale", che dovranno rispettare degli obblighi di trasparenza e le normative europee relative al diritto d'autore. I sistemi considerati "ad alto rischio" saranno soggetti a requisiti ben più severi. Questi includono i sistemi utilizzati, ad esempio, nelle infrastrutture critiche come l'istruzione, le risorse umane o il mantenimento dell'ordine pubblico. Inoltre, il regolamento vieta alcune applicazioni basate sull'IA, come i sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili e l'estrazione non mirata di immagini del volto di individui su Internet o tramite videosorveglianza per creare banche dati di riconoscimento facciale[140].

Infatti, l'AI Act adotta un approccio basato sul rischio (*risk-based approach*) che proibisce la diffusione di sistemi di intelligenza artificiale che

---

[139] M. IPPOLITO, *Le cooperative di dati nella pubblica amministrazione italiana: alcune riflessioni in punto di valorizzazione dei dati alla luce del Data Governance Act e dell'AI Act*, in *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, a cura di F. BRAVO, Torino, Giappichelli, 2024, 545-576.

[140] LÉGIPRESSE, *Publication de l'AI Act : la CNIL émet des premiers éléments d'information et rappelle son rôle de promotion d'une IA respectueuse des droits des personnes sur leurs données*, in *Légipresse*, 2024, 401.

comportano rischi inaccettabili e impone requisiti specifici ai sistemi di IA ad alto rischio, lasciando i sistemi di IA che presentano rischi bassi o minimi sostanzialmente liberi da oneri. Per ridurre i rischi associati ai sistemi di intelligenza artificiale ad alto rischio, i fornitori sono tenuti a rispettare i requisiti stabiliti nel Titolo 2. Tuttavia, l'AI Act riconosce che ciò potrebbe non essere sufficiente per abbattere tutti i rischi a un livello accettabile. Anche se i fornitori si attengono a tali requisiti, alcuni rischi potrebbero comunque persistere. In questo contesto, l'articolo 9 svolge un ruolo fondamentale, poiché si prefigge di garantire che i fornitori vadano a identificare questi rischi e adottino misure aggiuntive per ridurli ad un livello accettabile[141].

Qui si inseriscono la cosiddetta valutazione d'impatto sui diritti fondamentali (ovvero la *Fundamental Rights Impact Assessment*, sintetizzabile con l'acronimo FRIA), obbligo che il Regolamento pone in capo ai deployer e che ha per finalità quelle di valutare le categorie di persone fisiche e gruppi verosimilmente interessati dall'uso del sistema, la conformità del sistema con il diritto europeo e nazionale in materia di diritti fondamentali e l'impatto ragionevolmente prevedibile sui medesimi. La cosiddetta valutazione di conformità (ovvero la *conformity assessment*), prevista invece per obbligo attribuito dal Regolamento ai provider, ha il compito di presupporre un'analisi di conformità del sistema di IA rispetto ai requisiti richiesti dall'AI Act. La procedura di valutazione dovrà essere contraddistinta dalle seguenti quattro fasi: (i) identificazione e analisi dei rischi noti e prevedibili associati a ciascun sistema; (ii) stima e valutazione dei rischi che possono emergere quando il sistema è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile; (iii) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio

[141] J. SCHUETT, *Risk management in the artificial intelligence act*, in *European Journal of Risk Regulation*, 2024, 15(2), 367-385.

successivo all'immissione sul mercato; (iv) adozione di adeguate misure di gestione dei rischi che tengono in debita considerazione gli effetti e le possibili interazioni derivanti dall'applicazione combinata degli elementi indicati sopra alla luce dello stato dell'arte generalmente riconosciuto[142].

Si ricorda che non tutte le applicazioni dell'IA implicano l'uso di dati personali, e quindi i rischi sono da valutare in un'ottica di analisi caso per caso. Tuttavia, in questo momento particolare dell'evoluzione tecnologica è sempre più difficile effettuare una distinzione tra dati personali e dati anonimi. La presenza di "dati misti" – insiemi di dati personali e non personali spesso inseparabili – complica la gestione delle informazioni. L'innovazione tecnologica sta, come accennato, riducendo quella che era la distinzione tradizionale tra dati personali e non, poiché le capacità di analisi avanzata permettono di ottenere informazioni identificative anche da dati apparentemente anonimi. Questa evoluzione amplia il concetto di dato personale, estendendolo a contesti dalla natura sempre più varia[143].

In questo contesto non deve sorprendere che il citato "*risk-based approach*" sia particolarmente funzionale agli scopi dell'Unione Europea, che da sempre è alla ricerca del difficile equilibrio tra l'elevata protezione dei diritti e l'obiettivo primario della crescita economica e della creazione del mercato unico; a dimostrazione di ciò è il fatto che il modello basato sulla gestione del rischio abbia ispirato in parte la redazione del GDPR. In generale, la tutela dei dati personali nei trattamenti svolti mediante strumenti algoritmici rappresenta uno dei tanti principi di governance dell'IA. Nelle Linee Guida "*Ethics guidelines for trustworthy AI"* del 2019, la Commissione UE affermava che "*La trasparenza è un requisito fondamentale per garantire*

[142] P. FALLETA e A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di informatica e diritto*, 2024, 6(1), 119-137.
[143] C. COLAPIETRO e A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal-Rivista di BioDiritto*, 2020, 3, 359-387.

che il sistema di AI non sia viziato da bias. I sistemi di Intelligenza Artificiale utilizzati per prendere decisioni che riguardano gli individui sono soggetti al principio di 'diritto alla spiegazione': devono poter esplicitare la logica di funzionamento dei modelli che hanno generato". Il principio di trasparenza rappresenta uno dei pilastri della regolazione dei sistemi di Intelligenza Artificiale, ed è strettamente connesso alla nozione di *explainability*. Quest'ultima presuppone che siano trasparenti non solo gli output del sistema, ma anche gli elementi che ne costituiscono l'ossatura: i dati impiegati, l'architettura del sistema e i modelli di business sottesi alla sua implementazione. Affinché un sistema di IA possa essere effettivamente spiegabile, è necessario che i dati e i processi che conducono alla decisione siano adeguatamente tracciabili e documentabili. Ciò implica la possibilità di ricostruire, in modo intelligibile e verificabile, sia i passaggi tecnici (ad esempio le fasi di raccolta, etichettatura e trattamento dei dati), sia le scelte algoritmiche che orientano il funzionamento del sistema. L'*explainability*, pertanto, si fonda su una duplice dimensione: da un lato, la comprensibilità dei meccanismi tecnici che caratterizzano il funzionamento del sistema; dall'altro, la trasparenza delle decisioni umane che intervengono nel ciclo di vita dell'IA, e che ne influenzano l'adozione, la supervisione e l'uso concreto[144]. Si collega a quanto affermato un'analisi, interessante e necessaria, relativa al ruolo dell'art. 22 del GDPR, il quale riprende a sua volta l'art. 15 della precedente direttiva 95/46/CE, e che afferma che "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*". Questa norma si occupa di esprimere

[144] F. LORÈ e P. MUSACCHIO, *Intelligenza Artificiale, tra profili di responsabilità e protezione dei dati personali: aspetti de jure condito e prospettive de jure condendo*, in *Amministrativ@mente-Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2024, 1, 27-70.

un principio generale di grandissima importanza con riferimento ai sistemi di trattamento automatico dei dati, tra i quali si inseriscono quelli di IA: nessuna decisione che interferisca significativamente con una persona può essere presa "unicamente", *solely* (nel testo inglese), da un algoritmo (in corrispondenza, dunque, al principio di "non esclusività"). Questa regola, per il suo tenore testuale, permetterebbe di risolvere anticipatamente moltissime delle possibili controversie sull'utilizzo di algoritmi decisionali (un esempio possibile è quello relativo al settore della giustizia). Se il soggetto passivo, influenzato da un determinato trattamento, può in ogni momento chiedere di non essere sottoposto a una decisione automatizzata, ciò comporta che il sistema di intelligenza artificiale debba essere progettato in modo tale da permettere, sempre e comunque, un intervento umano; vale a dire l'intervento di un soggetto con piena capacità giuridica, dotato del potere di escludere l'operato della macchina e di assumere in prima persona le relative decisioni[145].

I sistemi di intelligenza artificiale sono all'avanguardia del progresso tecnologico, con l'IA generativa che guida l'innovazione in numerosi ambiti, dall'elaborazione del linguaggio naturale alla generazione di immagini. Tuttavia, l'efficacia e la funzionalità di tali sistemi dipendono in larga misura dalla qualità e dalla quantità dei dati utilizzati durante la fase di addestramento.

Nella sua Opinione del 17 dicembre 2024, il Comitato europeo per la protezione dei dati (EDPB) fornisce diverse indicazioni sul trattamento di dati personali tramite intelligenza artificiale. Il Parere pone l'accento sull'importanza delle aspettative ragionevoli degli interessati nell'ambito del test di bilanciamento. In questo contesto, elementi quali le informazioni fornite agli interessati e le circostanze specifiche del trattamento assumono

[145] G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, 5, 1193-1213.

un ruolo determinante nel valutare la capacità degli individui di prevedere ragionevolmente che i propri dati personali siano oggetto di trattamento. Tra i fattori contestuali rilevanti figurano, ad esempio, l'eventuale accessibilità pubblica dei dati, la natura della relazione tra l'interessato e il titolare del trattamento (nonché l'eventuale esistenza di un legame tra di essi), la tipologia di servizio coinvolto, le modalità di raccolta dei dati, la loro fonte (come il sito web o il servizio da cui provengono e le relative impostazioni sulla privacy), le possibili applicazioni future del modello e persino il fatto che gli interessati siano o meno consapevoli della disponibilità online dei propri dati personali[146].

La pubblicazione da parte della *Commission Nationale de l'Informatique et des Libertés* (CNIL) francese, in data 16 ottobre 2023, di una consultazione dedicata all'allineamento tra GDPR e AI Act, nonché alla creazione di dataset per l'intelligenza artificiale, evidenzia il ruolo centrale del GDPR come pilastro per un "approccio responsabile e innovativo" allo sviluppo dell'AI. Tale iniziativa dimostra come il quadro normativo europeo in materia di protezione dei dati personali possa costituire non un ostacolo, ma un supporto essenziale per una regolazione etica e sostenibile delle tecnologie emergenti.

In quest'ottica, è fondamentale che gli operatori adottino sistematicamente strumenti di valutazione dei rischi come la *Data Protection Impact Assessment* (DPIA), prevista dall'art. 35 del GDPR, e l'*AI Impact Assessment* (AIIA), introdotta dall'art. 29 dell'AI Act. Sarebbe auspicabile che queste valutazioni venissero integrate e redatte congiuntamente, al fine di fornire un'analisi completa e coerente delle implicazioni etico-giuridiche connesse all'impiego dell'intelligenza artificiale. Si ricorda, peraltro, che il GDPR già impone al titolare del trattamento l'obbligo di effettuare una DPIA

[146] J. ARNAL, AI at Risk in the EU: It's Not Regulation, It's Implementation, in *European Journal of Risk Regulation*, 2025, 1-10.

nei casi in cui il trattamento comporti l'uso di nuove tecnologie, rafforzando così l'interconnessione normativa tra i due strumenti regolatori[147].

Non è opinabile, dunque, che la diffusione di sistemi di intelligenza artificiale abbia creato un fenomeno dalle problematiche molto complesse. Essendo la circolazione dei dati molto estesa e poco controllabile a livello numerico, il controllo dell'origine dei dati risulta quanto mai più difficoltoso; pertanto, è spesso impossibile garantire tutte le tutele attribuite alla persona[148]. Attualmente, le tecnologie più innovative nel settore dell'intelligenza artificiale sono nel possesso degli Stati Uniti e della Cina, con il risultato che l'Unione Europea si trovi in difetto nello sfruttamento economico di questo settore. In aggiunta, tali sistemi sono così sofisticati che, di fatto, sono capaci non solo di comprendere l'evoluzione del gusto degli utenti, e, entro certi limiti, anche di prevedere eventi futuri, come l'esito di talune tornate elettorali o lo sviluppo geografico di determinate pandemie, risultando particolarmente strategici[149].

1.6.2 La governance dell'intelligenza artificiale

In mancanza della creazione di un'agenzia internazionale sul modello dell'Agenzia internazionale per l'energia atomica (AIEA), gli emendamenti parlamentari hanno proposto una nuova governance per l'IA, ispirata sia dal Digital Services Act (DSA) sia dal Regolamento generale sulla protezione dei dati (GDPR), con l'istituzione di un Ufficio europeo per l'IA (*AI Office*), che sostituisce il comitato previsto nella versione iniziale del testo. Questo ufficio avrà competenze estese, sarà dotato di personalità giuridica, e sarà affiancato

[147] A. LOMBARDI, *Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra GDPR e AI Act | Data protection regulation and artificial intelligence regulation: relationships, similarities and differences between GDPR and AI Act*, in *European Journal of Privacy Law & Technologies*, 2023, (2), 240-252.
[148] V. V. G. VESCIO DI MARTIRANO, *La governance dei dati personali e potere dispositivo dell'interessato*, Milano, Giuffrè, 2024.
[149] G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, 5, 1193-1213.

da poteri accresciuti della Commissione europea. Le funzioni di questo ufficio sono delineate in modo significativo nel nuovo articolo 56, e consistono in particolare nel garantire un'effettiva attuazione dell'AI Act e una cooperazione efficace con e tra le autorità di regolazione nazionali per tale attuazione[150].

Nel contesto della governance dell'Intelligenza Artificiale in ambito europeo, i primi orientamenti significativi si rinvengono in due documenti fondamentali della Commissione Europea: la Comunicazione del 25 aprile 2018, intitolata *L'intelligenza artificiale per l'Europa*, e le *Ethics Guidelines for Trustworthy AI*, redatte dallo *Independent High-Level Expert Group on Artificial Intelligence*. Le linee guida etiche, che sono stata poi successivamente riprese nel *Libro Bianco sull'intelligenza artificiale* del 19 febbraio 2020, rappresentano un tassello essenziale nella costruzione di un quadro normativo e valoriale per lo sviluppo dell'IA nell'Unione.

Le istituzioni europee hanno perseguito l'obiettivo di promuovere un'Intelligenza Artificiale sicura, affidabile e conforme ai principi fondanti dell'ordinamento europeo, in modo da coniugare l'innovazione tecnologica con la tutela dei diritti fondamentali e dei valori dell'Unione. In questa prospettiva, si punta alla creazione di un autentico *ecosistema di fiducia*, in cui l'IA non solo operi nel rispetto della legalità, ma osservi anche principi etici, evitando impatti negativi indesiderati. L'attenzione è rivolta, in particolare, a un impiego dell'IA che sia di supporto alle capacità umane, senza sostituirle, e che sia pienamente accessibile, anche alle persone con disabilità.

A rafforzare l'orientamento normativo indicato, il Parlamento Europeo ha approvato, il 20 ottobre 2020, tre risoluzioni concernenti rispettivamente l'etica, la responsabilità e la proprietà intellettuale dei sistemi

[150] J. SÉNÉCHAL, *Vote des parlementaires européens sur l'AI Act : vers une réglementation accrue des IA, des modèles de fondation et des IA génératives, s'inspirant du DSA, du Data Act et du RGPD ?*, in *Dalloz actualité*, 2023.

di IA, accompagnate da una quarta risoluzione specificamente dedicata ai sistemi d'arma autonomi letali[151].

Per quanto riguarda invece il sistema complessivo di governance delineato dal regolamento sull'intelligenza artificiale, questo si sviluppa su due livelli distinti ma interconnessi: il livello sovranazionale e quello nazionale, con l'intento di garantire una gestione efficace e coordinata delle questioni relative all'IA in ambito europeo. A livello sovranazionale, il regolamento prevede la creazione di quattro nuove strutture, che svolgono funzioni specifiche e si integrano tra loro per il monitoraggio e l'attuazione delle politiche riguardanti l'intelligenza artificiale: il primo di questi organi è l'Ufficio per l'Intelligenza Artificiale (*AI Office*) presso la Commissione Europea, recentemente istituito con la decisione C/2024/390 del 24 gennaio 2024, seguito dal Comitato europeo per l'IA (*European AI Board*), che è composto da rappresentanti degli Stati membri e ha il compito di coordinare le azioni tra i vari Stati membri; accanto a queste due strutture, vi è l'Advisory Forum, che include gli stakeholders, e il Comitato Scientifico, formato da esperti scientifici scelti dalla Commissione, entrambi con l'obiettivo di fornire consulenza tecnica e orientamenti strategici per l'implementazione del regolamento.

A livello nazionale, la governance si fonda su un sistema di controllo che include un'autorità di notifica e un'autorità di vigilanza del mercato, che operano in conformità con il regolamento (UE) 2019/1020, con l'obiettivo di garantire che le normative europee vengano rispettate e applicate correttamente sui mercati nazionali, creando così un quadro normativo ben

[151] F. LORÈ e P. MUSACCHIO, *Intelligenza Artificiale, tra profili di responsabilità e protezione dei dati personali: aspetti de jure condito e prospettive de jure condendo*, in *Amministrativ@mente-Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2024, 1, 27-70.

strutturato e sinergico che integra gli aspetti sovranazionali e nazionali nella gestione dell'intelligenza artificiale[152].

Il recente dibattito internazionale sulla corporate governance sembra convergere verso un consenso diffuso sull'impatto significativo che la digitalizzazione delle imprese e l'adozione di strumenti di intelligenza artificiale stanno avendo, e avranno sempre più, sul diritto societario e sulla gestione della corporate governance.

Il tema dell'impatto dell'intelligenza artificiale sulle imprese si colloca in un contesto più ampio, segnato da due elementi centrali. Da un lato, emergono le sfide complesse e in gran parte inedite che l'utilizzo sempre più esteso e invasivo delle nuove tecnologie pone al diritto, dall'altro, si osserva l'influenza crescente dell'intelligenza artificiale sulla società nel suo complesso, non solo intesa come ambito organizzativo (Gesellschaft), ma anche come comunità di relazioni sociali più ampie (Gemeinschaft), ossia la *Wider Society* rispetto alla sola dimensione aziendale rappresentata dalla Company o dalla Corporation[153].

Questi due livelli risultano strettamente interconnessi. Se oggi la nostra società, in senso ampio, è fortemente influenzata dagli algoritmi, tali

---

[152] S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE*, 2024, 2, 1-20.

[153] "*ll concetto originario, quello di Gemeinschaft, è stato introdotto nella letteratura sociologica da Ferdinand Tönnies. […]Tönnies usava la rappresentazione concettuale del predominante modo di vita passato e lo contrapponeva con un altro concetto rappresentante il modo di vivere presente, la Gesellschaft, solitamente tradotta in questo contesto come "società" . Quest'ultima nella versione di Tönnies si riferisce a un tipo di vita sociale fredda, impersonale e frammentata. La "società" ai suoi occhi mancava di coesione; gli esseri umani erano tra loro relativamente isolati; gli attriti e i conflitti erano frequenti. La vita di comunità, al contrario, è più calda, più familiare e affettuosa. Solidarietà e armonia, unità di intenti e cooperazione, assicurati da una forte tradizione, vi sono maggiormente presenti. La dicotomia comunità-società, in altre parole, come quella rurale-urbano, ha dei toni romantici. Riflette, almeno nella sua versione iniziale, il malcontento e la sofferenza connessi alla crescente urbanizzazione e industrializzazione; tradisce una certa nostalgia che preme per l'inversione di questa tendenza, per il ritorno a uno stadio precedente dello sviluppo delle società in cui la vita era più semplice e sembrava possedere tutte quelle desiderabili qualità oggi perdute. Per un certo periodo, "comunità" diventa il simbolo di tutte queste qualità."* Da: N. ELIAS, A. PERULLI E J. GOODWIN, *Verso una teoria delle comunità*, in *Cambio: rivista sulle trasformazioni sociali*, 2013, 6, 173-196.

sistemi sono ormai integrati nei processi delle grandi imprese societarie, rappresentando in alcuni casi il loro nucleo operativo. Questo è evidente, ad esempio, nelle grandi multinazionali dell'*information technology*, le cosiddette GAFAM (Google, Amazon, Facebook, Apple, Microsoft), ormai ai vertici delle società più capitalizzate al mondo. Oltre alle GAFAM, altre piattaforme digitali di rilevanza globale, come Ali Baba, Baidu e Tencent, giocano un ruolo essenziale, insieme a realtà di dimensioni minori ma comunque influenti, come Netflix. Tali attori evidenziano il peso crescente dell'intelligenza artificiale non solo nella trasformazione delle logiche aziendali, ma anche nella ridefinizione delle dinamiche sociali e culturali a livello planetario[154].

La questione sta assumendo un'importanza crescente in relazione alla tipologia di impiego con cui l'impresa decide di integrare l'intelligenza artificiale nel proprio contesto organizzativo e gestionale. In altre parole, a seconda del modo in cui questa tecnologia interagisce con la realtà societaria, si determinano diverse modalità di interferenza, che si possono configurare in tre principali approcci[155]:

- Utilizzo dell'intelligenza artificiale come strumento di supporto e di risultato nell'attività dell'impresa;
- Applicazione dell'intelligenza artificiale con una visione esterna riguardante il funzionamento della società;
- Uso dell'intelligenza artificiale con un approccio interno, impiegando gli strumenti di IA per l'organizzazione e il funzionamento interno dell'impresa.

La governance dell'IA si basa su regole formali (inclusi atti legislativi e regolamenti vincolanti) così come su principi volontari che hanno lo scopo

[154] M. RESCIGNO, *L'impresa nell'era dell'intelligenza artificiale: un'evoluzione tranquilla o nulla sarà più lo stesso?*, Milano, Giuffrè Francis Lefebvre, 2023, 13-14.
[155] A. DEL FORNO, *L'intelligenza artificiale nei processi gestori dell'impresa*, in *European Journal of Privacy Law & Technologies*, 2022, 2, 119-135.

di guidare i professionisti nella loro ricerca, sviluppo e manutenzione dei sistemi di IA. In sostanza, il quadro normativo può supportare i professionisti dell'IA nella formulazione delle loro strategie e nelle operazioni quotidiane. Le aziende sono tenute a comunicare le proprie politiche sulla privacy dei dati ai rispettivi interessati. Devono rassicurare i consumatori sul fatto che i dati raccolti con il loro consenso siano protetti e hanno l'obbligo di informarli che tali informazioni potranno essere utilizzate per migliorare i servizi personalizzati a loro destinati. Le big tech, tuttavia, incentivano strategicamente i consumatori a condividere informazioni sensibili, offrendo in cambio servizi personalizzati migliorati o altri tipi di vantaggi. In ogni caso, ai consumatori deve essere garantito l'accesso ai propri dati, insieme a un maggiore controllo (o ad altre opzioni ragionevoli) su come gestire le proprie informazioni personali[156]. In questo contesto si parla di Intelligenza Artificiale Responsabile (RAI, *Responsible Artificial Intelligence*). Il termine si riferisce allo sviluppo etico dei sistemi di intelligenza artificiale, con l'obiettivo di generare benefici per gli esseri umani, la società e l'ambiente. Il concetto di RAI ha suscitato un notevole interesse da parte di governi, organizzazioni, aziende e società in generale. Tale sviluppo rappresenta una soluzione positiva poiché, sebbene l'intelligenza artificiale possieda un enorme potenziale per affrontare sfide concrete del mondo reale, persistono serie preoccupazioni circa le capacità di agire in modo etico e di prendere decisioni in maniera responsabile[157].

Anche nel settore pubblico, lo sviluppo e l'implementazione dell'intelligenza artificiale non possono essere considerati separatamente dal più ampio contesto della trasformazione digitale dell'azione amministrativa. L'IA si inserisce infatti in un modello di nuova governance pubblica, che

[156] M. A. CAMILLERI, *Artificial intelligence governance: Ethical considerations and implications for social responsibility*, in *Expert Systems*, 2024, 41(7).
[157] Q. LU et al., *Responsible AI pattern catalogue: A collection of best practices for AI governance and engineering*, in *ACM Computing Surveys*, 2024, 56(7), 1-35.

implica la necessità di connettere la sua integrazione con una cultura della trasformazione, la quale deve permeare e caratterizzare l'intera organizzazione amministrativa[158]. Secondo le analisi di D. Marongiu, tuttavia, l'approccio giuridico all'automazione amministrativa mediata da intelligenze artificiali deve necessariamente differenziarsi rispetto a quello applicabile ai soggetti privati. La trasposizione di strumenti e pratiche già consolidate in contesti non istituzionali nell'ambito pubblicistico richiede infatti precauzioni, cautele e attenzioni amplificate. In particolare, il passaggio dall'informatica tradizionale all'impiego dell'intelligenza artificiale per l'esercizio del potere pubblico comporta una riduzione del controllo diretto della pubblica amministrazione sull'azione del sistema. Se il software è in grado di apprendere e auto-modificare i processi attraverso cui produce output, affinando autonomamente le proprie capacità, esso può operare al di là delle regole definite al momento della programmazione iniziale. Questo fenomeno ha evidenti implicazioni su temi di rilevanza fondamentali quali il rispetto delle garanzie procedimentali, l'imputabilità delle decisioni e la responsabilità della pubblica amministrazione. In conclusione, risulta opportuno porre particolare attenzione nel definire con chiarezza i limiti entro i quali l'uso delle intelligenze artificiali è ammissibile nella sfera pubblicistica e amministrativa[159].

Tra le aree di applicazione più importanti delle attuali tecnologie di intelligenza artificiale vi è la condivisione dei dati, ovvero la messa a disposizione di dati che hanno la loro origine in processi industriali o sociali di diversa natura. È utile citare i processi di dematerializzazione che procedono attraverso la digitalizzazione e i documenti cartacei dei grandi archivi e alla loro catalogazione in sistemi di informazione digitali che siano

[158] E. M. MENÉNDEZ SEBASTIÁN, *L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie*, in *CERIDAP*, 2023, 2, 66-84.
[159] D. MARONGIU, *L'intelligenza artificiale "istituzionale": limiti (attuali) e potenzialità*, in *European Review of Digital Administration & Law*, 2020, 1, 37-53.

sia interrogabili che aperti alla ricerca di documenti e analisi statistiche (questo avviene per esempio in diversi enti pubblici, come ospedali per descrivere l'epidemiologia dei fenomeni patologici). L'IA pertanto può aiutare sia a recuperare dati che altrimenti resterebbero inutilizzati (come nel caso di archivi clinici), sia l'utilizzo di metadati diffusi su banche dati online[160].

[160] R. BASILI, *Interoperabilità dei dati, metodologie di condivisione e prospettive: opportunità e rischi*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 33-64.

CAPITOLO II
MERCATO DEI DATI PERSONALI TRA COMMERCIALIZZAZIONE E PROTEZIONE

Sommario: 2.1 Big Data e mercato digitale – 2.2 La mercificazione dei dati secondo la lettura "patrimonialistica" – 2.3 Il consenso e le sue fragilità nel mercato dei dati – 2.4 Proprietà, controllo e uso dei dati: modelli normativi a confronto – 2.5 Il diritto alla portabilità dei dati tra datification e data protection by design – 2.6 "Interoperable Europe Act" e il Mercato Unico Digitale Europeo

2.1 Big Data e mercato digitale

In questo capitolo si richiama il quadro normativo di riferimento, evidenziando le potenzialità di sviluppo economico connesse all'utilizzo dei dati, in particolare attraverso la loro raccolta e successiva monetizzazione e, parallelamente, si affrontano problematiche inerenti alla tutela dei dati personali.

L'ordinamento giuridico europeo, dopo un lento percorso che ha condotto al riconoscimento formale del diritto alla protezione dei dati personali nella Carta dei diritti fondamentali dell'UE (art. 8), sta ora intraprendendo direzioni volte a incentivare il mercato dei dati personali, con l'obiettivo di non far perdere competitività alle imprese europee rispetto alle logiche proprietarie che invece caratterizzano i mercati extraeuropei[161].

Se il diffuso impiego degli strumenti digitali porta con sé la promessa di semplificare i processi decisionali all'interno delle organizzazioni

[161] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, 199-256.

complesse, come aziende ed enti pubblici, esso pone altresì dubbi e incertezze sull'impatto che tali strumenti (spesso imprevedibili e indipendenti rispetto agli operatori umani) possono avere sui diritti e sulle libertà degli interessati (persone fisiche), segnatamente in materia di protezione dei dati personali. Infatti, il funzionamento di nuove e sofisticate tecnologie digitali presuppone spesso l'impiego di ampi dataset, con conseguente trattamento di dati personali; in tali casi è necessario che i titolari adeguino gli strumenti informatici agli obblighi previsti dal GDPR[162]. Se a metà degli anni 2000 destava ancora sorpresa il fatto che l'ecosistema digitale si reggesse sull'apparente gratuità di numerosi servizi, oggi i consumatori (soprattutto dopo i più recenti scandali che hanno coinvolto il colosso di Menlo Park) stanno maturando una maggiore consapevolezza riguardo al modello economico delle grandi piattaforme online. È ormai evidente, infatti, che una parte significativa dei loro profitti derivi dalla raccolta e dalla successiva monetizzazione dei dati personali degli utenti[163].

È ampiamente riconosciuta la diffusione di un modello di business[164] cosiddetto *zero-price*, che prevede l'erogazione di servizi a titolo gratuito, senza la previsione di un corrispettivo pecuniario, subordinatamente all'acquisizione del consenso per il trattamento dei dati personali degli utenti. Tale modello risulta particolarmente prevalente nelle interazioni online, pur non essendo esclusivamente ad esse circoscritto, ed è stato favorito dal progresso delle nuove tecnologie, che consentono tecniche sempre più

[162] M. BIANCHINI, G. GASPARRI, G. RESTA et al., *Gli sviluppi tecnologici del diritto societario (Quaderno giuridico n. 23)*, Consob, maggio 2022.
[163] J. ARPETTI, *Economia della privacy: una rassegna della letteratura*, in *Rivista di diritto dei media*, 2018, 2, 267-297.
[164] Per una definizione di modello di business si può far riferimento alla descrizione di G. Donna: "Le numerose definizioni proposte, pure differenziandosi sul piano lessicale, convergono nell'identificare nel modello di business l'illustrazione di come un'azienda intende creare valore. "*Business models are stories that explains how enterprises work … to deliver value to customers, entice customers to pay for value and convert those payments to profits*"" in G. DONNA, *Modello di business, patrimonio strategico e creazione di valore*, in *Impresa Progetto*, 2018, 2, 11-23.

pervasive e sofisticate di raccolta, monitoraggio e sfruttamento dei dati personali. A differenza dei modelli *zero-price*, nei cosiddetti modelli di *personal data economy* le imprese che trattano dati personali prevedono una forma esplicita di remunerazione per gli utenti, riconoscendo loro una quota, per quanto minima, del valore economico generato attraverso la profilazione o altre attività di marketing.

Un caso significativo è quello della startup newyorkese Datacoup, fondata da Matt Hogan, che offriva agli utenti circa otto dollari al mese in cambio dell'accesso ai propri dati provenienti dai social network e dai movimenti delle carte di credito. L'azienda sosteneva di procedere alla successiva vendita dei dati in forma anonimizzata, così da evitare l'identificazione diretta degli interessati. Un ulteriore esempio può essere rintracciato nella società californiana Doc.ai, che consente agli utenti di partecipare a progetti di ricerca in ambito sanitario prevedendo, come forma di compenso, l'attribuzione di punti convertibili in buoni regalo, ad esempio utilizzabili su Amazon. In tali ipotesi, il trasferimento dei dati personali assume dunque la funzione di una vera e propria controprestazione economica, rivelando come l'informazione personale possa ormai costituire un bene dotato di valore di scambio nel mercato digitale[165].

Nel contesto europeo, tuttavia, si applicano ad ogni trattamento di dati personali le basi giuridiche, ai sensi dell'art. 6 del GDPR, riportate di seguito: il consenso dell'interessato, l'esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato, l'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento, la tutela degli interessi vitali dell'interessato o di un'altra persona fisica, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, e il

[165] C. A. TROVATO, *Commercializzazione dei dati personali: limiti e condizioni*, in *Legal Tech, Big Data e contratti smart per professionisti e imprese,* a cura di S. MARTINELLI, C. ROSSI CHAUVENET, Wolters Kluwer, Milano, 2022, 199-217.

legittimo interesse perseguito dal titolare del trattamento o da terzi, nel rispetto dei diritti e delle libertà fondamentali dell'interessato. Il consenso, anche se libero ed esplicito, non permette di trasferire la proprietà dei propri dati personali, ma ne consente l'utilizzo che può essere sempre soggetto a limiti o revoche.

La fornitura di beni e servizi costituisce un'occasione preziosa per accedere alle potenzialità economiche dei cosiddetti big data[166]. L'*Autorité de la Concurrence* in Francia e il *Bundeskartellamt* in Germania hanno congiuntamente sottolineato come la creazione di valore sia strettamente connessa allo sviluppo di nuove tecniche in grado di estrarre "informazioni preziose da enormi quantità di dati (spesso non strutturati)". In questo contesto, i *big data* risultano strettamente collegati ai "*big analytics*", ovvero alla capacità dei sistemi informatici di affrontare problemi complessi attraverso l'analisi di grandi volumi di dati grazie all'uso di algoritmi avanzati[167]. Come per diverse altre espressioni nel campo delle tecnologie digitali recenti, il termine "Big Data" si utilizza per indicare una metafora dello sviluppo della società dell'informazione. Esso risale al 2011, anno in cui il termine è stato utilizzato dal McKinsey Global Institute, che si è occupato di definire i big data come quei set di dati la cui dimensione supera la capacità di un database di acquisire, archiviare, gestire e analizzare dati e informazioni[168]. Un decennio prima, nel 2001, Laney[169] attraverso il modello di crescita tridimensionale delle "3 V": Volume, Velocità e Varietà, viene definito un punto di partenza utile al fine di identificare alcuni tratti da tenere

[166] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws*, 2019, 131-147.
[167] S. GOBBATO, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *Media Laws*, 2019, 148-161.
[168] G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy digitale*, a cura di E. TOSI, Milano, Giuffrè, 2019, 447-484.
[169] D. LANEY, *3D data management: Controlling data volume, velocity and variety*, META Group, 2001.

in considerazione nell'analisi del fenomeno dei dati legato alle peculiarità del web.

L'evoluzione dei Big Data Analytics ha posto in evidenza le criticità del tradizionale processo di categorizzazione dei dati, il quale appare ormai eccessivamente complesso e di ridotta efficacia. Sebbene la classificazione dei dati possa avvenire in una fase preliminare di ricognizione dei dataset, essa si rivela spesso di limitata utilità nella fase successiva al trattamento, soprattutto con l'impiego di strumenti avanzati di machine learning. È noto, infatti, che grazie all'utilizzo di algoritmi sempre più sofisticati, è oggi possibile inferire informazioni personali relative a un individuo anche a partire da dati originariamente non qualificabili come personali. Il celebre filosofo L. Floridi, da tempo discute delle potenzialità dei Big Data, sostenendo che in un mondo segnato da un sovraccarico informativo (*over-information*), l'interesse delle multinazionali e anche dei governi non è più concentrato sul targeting individuale, ovvero sulla profilazione del singolo soggetto, poiché ciò risulterebbe troppo complesso e scarsamente vantaggioso. Oggi la tattica prevalente è il group-targeting, ovvero la suddivisione delle persone in gruppi in base a preferenze comuni espresse o scelte compiute. Il gruppo, non solo sotto il profilo politico ma anche economico, risulta più influente dell'individuo. Per riflettere sulla privacy (così come su molte altre istituzioni giuridiche) in modo strutturalmente adeguato a un mondo che si spinge sempre più verso la sua dimensione virtuale, è necessario che il giurista sia in grado di dominare il pensiero sistemico e di adottare una visione autenticamente relazionale e collettiva dell'esperienza sociale[170].

Quando si parla di *economia della conoscenza* ciò che si intende è economia della conoscenza dei nostri dati personali, tale osservazione,

[170] L. MERLA, *Big Data e diritto: una sfida all'effettività*, in *Media Laws*, 2021, 1, 218-233.

all'interno di questa indagine, conferma che il prodotto di questo sistema economico siamo noi, insieme al complesso di dati che contribuiamo ad offrire ai voraci colossi stanziati nella Silicon Valley. L'economia globale risulta dunque una declinazione di quella digitale, e, seguendo questa logica, le tecnologie cosiddette "*disruptive*", dell'informazione e della comunicazione non costituiscono più un settore distinto ma diventano un fondamento soggiogante di tutti i sistemi economici innovativi moderni[171].

L'impiego degli algoritmi, applicati a ingenti volumi di dati, consente non solo di estrarre, ma anche di prevedere informazioni personali, talvolta attraverso la correlazione tra dataset eterogenei per origine e contenuto. In questo contesto, la distinzione tra dato personale e dato non personale risulta progressivamente più incerta, rendendo altresì sempre meno sostenibile l'applicazione di regimi giuridici distinti alle diverse tipologie di dati[172].

2.2 La mercificazione dei dati secondo la lettura "patrimonialistica"

Nel testo "*I dati personali nel diritto europeo*[173]", curato da V. Cuffaro, R. D'Orazio e V. Ricciuto, viene esaminata la disciplina introdotta dal Regolamento UE 2016/679 (GDPR) proponendo una innovativa prospettiva definita come "lettura patrimonialistica" del fenomeno del trattamento dei dati personali. Pur non essendone una sua alternativa diretta, tale visione si distingue dalla tradizionale lettura "personalistica" prevalente nella tradizione scientifica italiana, ed è capace di rispondere alle evoluzioni

[171] E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, Giuffrè, 2023.
[172] V. PAGNANELLI, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di informatica e diritto*, 2021, 3(1), 11-26.
[173] V. CUFFARO, R. D'ORAZIO e V. RICCIUTO, *I dati personali nel diritto europeo: Un'analisi della disciplina introdotta dal Regolamento UE 2016/679*, Giappichelli, 2018.

tecnologiche ed economiche che hanno trasformato il trattamento dei dati personali in un pilastro fondamentale del capitalismo digitale contemporaneo.

Questa interpretazione si basa sul riconoscimento di un fatto che è ormai diffuso: il processo di patrimonializzazione dei dati personali. I dati, perciò, non sono più semplici informazioni personali, ma sono considerati come una vera e propria merce, dotati di un loro valore economico che viene riconosciuto anche sul piano normativo. Nel contesto descritto in cui si parla di capitalismo digitale, i dati personali assumono lo status di beni giuridici, grazie all'applicazione di uno dei principi fondanti del diritto privato: il principio di patrimonialità. In questo modo[174] la lettura patrimonialistica riconosce ai dati personali un ruolo che risulta centrale nelle dinamiche del mercato e nella configurazione del sistema economico contemporaneo, evidenziando il loro valore sia per gli individui che per le imprese che operano nel settore del trattamento dei dati. Va ricordato innanzitutto che l'Unione Europea si è infatti caratterizzata sin dalle sue origini come una costruzione ispirata da finalità che erano prevalentemente di natura economica. Per conseguenza diretta ciò ha portato ad una maggiore attenzione e cura verso quelle che sono stabilite come libertà fondamentali di natura economica: la libera circolazione delle persone, la libertà di stabilimento, la libertà di prestazione dei servizi e la libera circolazione dei capitali. Un'ulteriore conseguenza piuttosto logica è stata che anche taluni diritti fondamentali, ad incominciare da quello alla privacy, venissero tutelati nella loro accezione patrimoniale o patrimonializzabile[175]. I dati personali costituiscono ricchezza e alimentano dunque l'economia digitale, a conferma di ciò, il d.lgs. 4 nov. 2021 n.173 ha introdotto all'interno del Codice del Consumo (d.lgs. 6 settembre 2005 n. 206) il Capo I bis denominato "*Dei contratti di fornitura*

[174] G. DI LORENZO e R. MESSINETTI, *Ordine giuridico ed evoluzione tecnologica, a proposito del recente libro su "i dati personali nel diritto europeo"*, in *NOMOS*, 2019, 3, 1-25.
[175] S., SICA, V., D'ANTONIO e G. M., RICCIO, *La nuova disciplina europea della privacy*, Wolters Kluwer, 2016.

di contenuto digitale e di servizi digitali". L'art 135 *octies* (*Ambito di applicazione e definizoni),* si occupa di contemplare la fattispecie dello scambio contenuti/servizi con dati personali a fronte del pagamento di una somma di denaro. Del contratto descritto, l'interessato (identificato anche come consumatore) risulta essere la parte debole, a cui, tuttavia, spettano una serie di diritti enunciati nel Capo III del GDPR, in cui trova riconoscimento il diritto a controllare la circolazione delle informazioni che lo riguardano. Lo sfruttamento economico dei dati resta comunque problematico, il *footprint* digitale dell'individuo rimane in mano alle *digital companies* che lo utilizzano per influenzare opinioni e comportamenti in tutti i settori dell'esistenza. Ciò avviene, ad esempio, attraverso la formazione di oligopoli che finiscono per alterare la leale competizione [176].

In questo contesto è compito del giurista rimanere vigile davanti alle strategie che permettono di mimetizzare le logiche di mercato che avanzano pretese anche nelle sfere private degli individui. Strategie di comportamento poco trasparenti inducono l'utente a condividere con le piattaforme le proprie informazioni, sottoforma di dati personali, di cui spesso non conoscono il valore reale, andando ad alimentare il cosiddetto "capitalismo della sorveglianza". La nostra Costituzione, all'art. 2. offre un orientamento "garantista" che rende il diritto alla protezione dei dati personali un diritto fondamentale indisponibile e che quindi non può essere oggetto di contratto. Il dato non dovrebbe quindi essere soggetto alla mercificazione poiché legato in maniera inscindibile alla persona fisica e al suo diritto all'autodeterminazione informativa, questo perché i dati personali rappresentano un bene giuridico prima di essere una risorsa economica. Se questo paradigma venisse a mancare assisteremmo ad una rifeudalizzazione dei rapporti sociali in cui è possibile cedere, attraverso i propri dati, la libertà.

[176] A. MORACE PINELLI, Introduzione, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 1-22.

Quella descritta è una battaglia irrinunciabile a tutela della libertà e dei diritti fondamentali, poiché il costrutto *privacy digitale* non può considerarsi come un ossimoro giuridico, ovvero una contraddizione in termini[177].

Secondo orientamenti di natura liberista, tuttavia, l'esercizio dei dati può essere messo a disposizione a determinate condizioni stabilite; infatti, nella società *data driven* il dato diventa uno strumento economico suscettibile di patrimonializzazione. A sostenere questo modello è anche la sentenza della Cassazione Adspray 2018[178], poiché essa nega che l'ordinamento vieti lo scambio di dati personali, ma ribadisce che questo debba essere frutto di un consenso libero ed espresso in assenza di coercizioni, per cui: "*è dunque senz'altro da escludere che il consenso possa dirsi specificamente, e dunque*

[177] E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, Giuffrè, 2023.

[178] Si verificava che la società commerciale Ad Spray s.r.l. offriva, tramite un portale di sua proprietà, un servizio gratuito di newsletter riguardante tematiche connesse alla finanza, al fisco e al lavoro. La ricezione della newsletter era subordinata all'iscrizione al servizio da parte dell'utente mediante l'inserimento delle proprie generalità e di un indirizzo email in un modulo digitale appositamente collocato nel sito. In fondo al modulo era presente una casella da selezionare per manifestare il consenso al trattamento dei dati personali, accompagnata da un link ipertestuale che, una volta cliccato, permetteva di consultare l'informativa sulla privacy e le finalità per cui i dati venivano raccolti, tra cui figurava genericamente l'utilizzo di tali dati per l'invio di comunicazioni promozionali e commerciali da parte di terzi. La struttura del sito, di proprietà della società che offriva il servizio di newsletter, comportava la manifestazione del consenso come condizione indispensabile per accedere al servizio. In particolare, la mancata selezione della casella impediva l'invio del modulo di iscrizione alla newsletter, generando la visualizzazione sullo schermo di un messaggio che avvertiva che il consenso era necessario per completare il processo di iscrizione. Una volta completata con successo l'iscrizione e accettata tale condizione, gli utenti iniziavano a ricevere messaggi email di natura promozionale su argomenti non collegati agli ambiti del fisco, finanza, lavoro e diritto, temi originariamente trattati dal sito. Di fronte all'aumento di messaggi indesiderati nella propria casella di posta elettronica, un iscritto alla newsletter ha presentato ricorso al Garante per la protezione dei dati personali, contestando la liceità della raccolta dati per violazione dei requisiti di libertà e specificità del consenso, richiesti ai fini della legittimità del trattamento dall'art. 23 del Codice Privacy del 2003, che all'epoca dei fatti regolava il trattamento dei dati personali. Pur sollevando il tema della validità del consenso, nella decisione del ricorso la Cassazione ha esaminato diversi profili della protezione dei dati personali, riguardanti sia i requisiti della manifestazione di volontà sia la classificazione delle operazioni che coinvolgono lo scambio tra servizi digitali e dati personali. F. CAGGIA, *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del "consenso rafforzato"*, in *I problemi dell'informazione nel diritto civile, oggi: studi in onore di Vincenzo Cuffaro*, a cura di M. D'AURIA, Roma Tre Press, 2022, 417-430.

anche liberamente, prestato in un'ipotesi in cui, ove gli effetti del consenso non siano indicati con completezza accanto ad una specifica 'spunta' apposta sulla relativa cartella di una pagina Web, ma siano invece descritti in altra pagina Web linkata alla prima, non vi sia contezza che l'interessato abbia consultato detta altra pagina, apponendo nuovamente una diversa 'spunta' finalizzata a manifestare il suo consenso."

La gratuità dei servizi, di natura solo apparente, induce la maggior parte degli utenti a cedere i propri dati in cambio del servizio. La monetizzazione dei dati personali, in senso stretto, si tramuterebbe in una patrimonializzazione della libertà che comporterebbe lo sviluppo di un sistema in cui la privacy può essere associata ad un lusso per pochi[179]. La maggior parte degli interessati non conosce affatto il valore dei propri dati personali e, in ogni caso, risulterebbe complicato attribuire loro un valore specifico. Tale asimmetria è amplificata dallo squilibrio tra le parti contrattuali, per cui l'utente si ritrova nella posizione di dover accettare le condizioni delle *BigTech* per accedere al servizio[180].

Citando studi di matrice sociologica, si sottolinea che la mercificazione delle persone, o la loro riduzione a materia prima, come afferma S. Zuboff, si riferisce al fenomeno in cui le persone sono trattate principalmente come risorse da sfruttare per fini economici o di controllo[181]. Gli algoritmi vengono criticati per il loro ruolo nell'utilizzo strumentale dell'esperienza quotidiana degli individui, trattata come una risorsa gratuita

---

[179] A. GHIGLIA, *Commerciabilità dei dati personali: condizioni e limiti alla monetizzazione della nostra identità digitale nel contesto italiano ed europeo*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024, 23-32.

[180] C. A. TROVATO, *Everything has its price? Una riflessione sull'ammissibilità delle pratiche di commercializzazione dei dati personali*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024, 301.

[181] S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.

da cui estrarre dati. Questi dati vengono poi trasformati in prodotti altamente predittivi, impiegati per influenzare e orientare i comportamenti delle persone in modo mirato[182]. Non sorprende quindi che sia stato evidenziato come sia del tutto legittimo affermare che le informazioni, oltre a supportare e ottimizzare gli scambi economici e le transazioni convenzionali, stiano assumendo il ruolo di un vero e proprio fattore di produzione, comparabile a terra, capitale e lavoro[183]. Inoltre, i broker di dati svolgono un ruolo centrale nell'economia dei dati e, più in generale, nel fenomeno del "capitalismo della sorveglianza". I data broker, più che semplici rivenditori di informazioni, fungono da facilitatori dello scambio di dati tra organizzazioni e contribuiscono alla creazione di veri e propri mercati dei dati dei consumatori. Tale processo incentiva ulteriormente pratiche di sorveglianza da parte di una vasta gamma di soggetti. In tal modo, questi attori riproducono ed estendono le logiche di "*commodification*" dell'audience, radicate nei processi storici di espansione del capitalismo. Gli utenti vengono trattati come merci, e la loro attività online diventa un lavoro inconsapevole a beneficio delle imprese digitali[184].

Ma quali sono le implicazioni giuridiche della mercificazione associata alla *datification* delle persone? Quali sono le conseguenze legali quando la mercificazione è incentivata, in maniera più o meno consapevole, dall'uso diffuso delle piattaforme digitali? Risulta impossibile al momento fornire una risposta definitiva ai quesiti posti, poiché la complessità del fenomeno della mercificazione associata alla "*datification*" delle persone è oggetto di dibattito e riflessioni giuridiche in evoluzione costante. La trasformazione dei dati personali in beni di valore economico, e la

[182] S. TIRIBELLI, *Oltre la privacy informazionale: libertà di scelta e di identità nell'era della profilazione algoritmica*, in *Itinerari*, LXI/2, 2022, 161-188.
[183] L. CALIFANO, *Come si governa la tecnologia digitale?*, in *Cultura giuridica e diritto vivente*, 2021, 8, 1-11.
[184] U. REVIGLIO, *The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview*, in *Internet Policy Review*, 11(3), 2022, 1-27.

conseguente mercificazione degli individui attraverso le loro tracce digitali, solleva molteplici questioni di stampo sia legale che etico che non possono essere pienamente risolte con una normativa univoca. In aggiunta a ciò, è utile ricordare che, nel regolamentare la tecnologia, è difficile non imbattersi nel cosiddetto dilemma di Collingridge[185]. Questo fenomeno descrive la situazione in cui, dal momento dell'emergere di un'innovazione tecnologica alla sua regolamentazione, passa molto tempo a causa di una certa esitazione dei regolatori, i quali non agiscono tempestivamente per mancanza di informazioni più specifiche sul funzionamento della tecnologia di riferimento. Pertanto, nel momento in cui tali informazioni diventano disponibili, le normative rischiano di essere già obsolete, poiché non più allineate con i progressi tecnologici. Ci troviamo, infatti, di fronte sia a un problema di mancanza di informazioni (il che significa che gli impatti non possono essere facilmente previsti fino a quando la tecnologia non è ampiamente sviluppata e utilizzata dalla popolazione), sia a un problema di potere (il controllo o il cambiamento diventano difficili quando la tecnologia è ormai profondamente radicata). Le iniziative regolamentari adottate finora dall'Unione, sebbene apprezzabili, non forniscono ancora una risposta completa alle sfide poste dalla mercificazione dei dati personali, incentivata, spesso inconsapevolmente, attraverso l'uso diffuso dei social network e dei motori di ricerca. Le tecnologie emergenti e l'economia basata sui dati, in particolare i modelli di business che si fondano sulla raccolta e l'analisi delle attività online degli utenti, hanno richiesto vari interventi da parte dell'Unione Europea per promuovere la libera circolazione dei dati personali, garantendo al contempo una protezione agli individui. A tal proposito, la normativa comunitaria, attraverso il GDPR, il Digital Services Act e il Digital Markets Act, mira a facilitare il flusso libero dei dati personali all'interno dell'Unione

[185] A. GENUS e A. STIRLING, *Collingridge and the dilemma of control: towards responsible and accountable innovation*, in *Research Policy*, 47(1), 2018, 61-69.

e il loro trasferimento verso paesi terzi e organizzazioni internazionali. La mercificazione, intesa come riduzione a materia prima delle persone attraverso la datificazione, è intimamente connessa con una sorveglianza di massa continua e pervasiva. Tale sorveglianza è resa possibile dalla capillare diffusione di Internet e, in particolare, dall'attività di piattaforme digitali predominanti come Google e Facebook. Questo fenomeno solleva importanti

questioni giuridiche relative alla tutela della privacy, alla protezione dei dati personali e alla conformità alle normative vigenti, quali il GDPR e altre leggi sulla protezione dei dati a livello globale. La raccolta, l'elaborazione e la commercializzazione dei dati personali senza un consenso esplicito rappresentano una violazione dei diritti fondamentali degli individui, incluso il diritto alla riservatezza[186].

2.3 Il consenso e le sue fragilità nel mercato dei dati

Nel 2017 un gruppo di studiosi della Stanford University ha condotto un esperimento destinato a diventare emblematico nel dibattito sulla tutela dei dati personali. A un gruppo di studenti universitari, che avevano dichiarato di attribuire grande importanza alla propria privacy, è stata offerta una pizza in cambio della condivisione di alcune informazioni personali. La maggior parte di essi ha accettato, rivelando così una significativa distanza tra le convinzioni dichiarate e i comportamenti effettivi. Da tale evidenza empirica è stato coniato il termine *privacy paradox*, utilizzato per descrivere la tendenza degli individui a sacrificare la propria riservatezza per benefici immediati, anche di scarso valore economico. Questo episodio, apparentemente banale, mostra con chiarezza quanto la percezione soggettiva della privacy sia spesso fragile

[186] R. CASO, *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Milano, Ledizioni, 2021, 1-364.

e condizionata da incentivi minimi, aprendo una riflessione più ampia sulla consapevolezza e sulla cultura della protezione dei dati nell'era digitale[187].

Le asimmetrie di potere si cristallizzano progressivamente nel rapporto tra le big tech titolari del trattamento e la stessa persona fisica interessata dal trattamento. Si registra dunque l'emergente progressiva fragilità del consenso della persona fisica nella società digitale, di fronte alla pervasività dei digital player globali e dei big data. Quello che sta avvenendo nel sistema attuale, è riconducibile al fenomeno per cui più aumenta la tecnologia del mercato più si affievolisce la capacità di prestazione del consenso attribuibile al singolo individuo[188]. Tuttavia, prendere una posizione su uno dei temi più spinosi e delicati della teoria dei rapporti giuridici nella società digitale e dunque riflettere sulla relazione concettuale e dogmatica tra consenso al trattamento dei dati personali e contratto risulta tanto interessante quanto difficile. Quando il consenso al trattamento dei dati personali si inserisce in un contesto in cui il dato stesso è considerato un valore e un bene economico, si pone il problema di stabilire se tale consenso assuma anche una valenza negoziale, fino al punto da poter essere inteso come elemento costitutivo di una vera e propria fattispecie contrattuale. Come sostiene V. Ricciuto, quando un interessato decide di fornire i propri dati personali per accedere a un servizio sta, di fatto, compiendo una scelta di natura economica. Su questo aspetto, il legislatore dell'Unione Europea ha posto negli ultimi anni una particolare attenzione, soprattutto nell'ambito della normativa a tutela dei consumatori. Non risulta sufficiente, infatti, che l'interessato presti il proprio consenso in senso formale (ossia che voglia l'atto): è altresì necessario che egli comprenda pienamente le implicazioni giuridiche ed economiche di tale scelta. Ciò include, ad esempio, la consapevolezza dello

[187] C. A. TROVATO, *Commercializzazione dei dati personali: limiti e condizioni*, in *Legal Tech, Big Data e contratti smart per professionisti e imprese,* a cura di S. MARTINELLI, C. ROSSI CHAUVENET, Wolters Kluwer, Milano, 2022, 199-217.
[188] E. TOSI, *Dati personali e contratto: un ossimoro apparente,* in *European Journal of Privacy Law & Technologies*, 2, 2023, 71-92.

scambio che avviene, degli obblighi assunti dal fornitore del servizio, nonché dell'attivazione delle tutele previste in ambito consumeristico[189].

Le attuali restrizioni sulla commerciabilità dei dati sono frutto delle normative vigenti in materia di protezione dei dati personali, con particolare attenzione alla regolamentazione dei requisiti per il consenso al trattamento, il quale, come già sottolineato, deve essere "libero". Come noto, tali disposizioni giuridiche bilanciano due interessi contrapposti: da un lato, la promozione della libera circolazione dei dati nel contesto di uno sviluppo del mercato unico dei dati; dall'altro, la salvaguardia dei dati personali, riconosciuta tra i diritti fondamentali nell'ordinamento dell'Unione Europea[190]. Occorre esaminare il secondo paragrafo dell'art. 7 GDPR, che disciplina i casi in cui il consenso al trattamento dei dati è prestato nell'ambito di una dichiarazione scritta che tratta anche altre questioni, ad esempio nella fornitura di servizi digitali rispetto al consenso a dati non necessari per l'esecuzione del contratto. Il GDPR prescrive che la richiesta del consenso sia chiaramente distinguibile dal resto, comprensibile e accessibile, con linguaggio semplice e chiaro. L'art. 7 stabilisce che nessuna parte della dichiarazione che violi il regolamento è vincolante, implicando l'invalidità del consenso.

Tale principio trova riscontro anche nella disciplina delle clausole abusive dei contratti dei consumatori (art. 6 dir. 93/13), ma non comporta l'invalidità automatica del contratto stesso, che rimane distinto dalla dichiarazione di consenso. In generale, né il GDPR né la dir. UE/2019/770 prevedono conseguenze specifiche dell'invalidità del consenso sul contratto. Tuttavia, un difetto di comprensibilità nella richiesta del consenso o nelle condizioni generali potrebbe rilevare ai fini della vessatorietà della clausola

[189] D. V. RICCIUTO, *Consenso al trattamento e contratto*, in *Persona e Mercato*, 2024, 13-26.

[190] S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *Media Laws*, 2019, 131-147.

contrattuale (art. 4 par. 2 dir. 93/13), soprattutto se riguarda l'indicazione dei dati personali di cui il consumatore autorizza il trattamento a scopi economici.

Non si tratta di un'automatica conseguenza della mancanza di chiarezza, ma uno squilibrio significativo dei diritti e obblighi a carico del consumatore può sussistere. La questione della vessatorietà può prescindere dal rapporto tra consenso al trattamento dei dati personali e consenso negoziale. La dottrina e la giurisprudenza hanno qualificato tali contratti in modi diversi: obbligo di consentire il trattamento, cessione dei diritti di sfruttamento economico dei dati, contratto atipico di cessione dati, contratto gratuito collegato al consenso, promessa condizionata o contratto oneroso a prestazioni corrispettive. Un difetto di chiarezza e comprensibilità delle condizioni generali, in particolare dell'individuazione dell'oggetto, può incidere sulla validità del contratto. L'invalidità contrattuale si invoca non solo per contrastare pretese esecutive, ma anche per verificare eventuali obblighi restitutori. La dottrina si è concentrata principalmente sul risarcimento del danno derivante da trattamento illecito basato su consenso invalido[191].

La Corte di Giustizia dell'Unione Europea[192] ha già avuto modo di scoraggiare l'uso dei cosiddetti *dark patterns,* ossia quelle pratiche che ostacolano la libera autodeterminazione dell'utente. In particolare, la Corte ha ribadito che, per essere valido, il consenso deve risultare da un'azione positiva e inequivocabile, distinta rispetto all'attività che l'utente intende compiere. In un caso specifico, una società tedesca aveva adottato una casella di spunta preselezionata tramite cui gli utenti, desiderosi di partecipare a giochi a premi, venivano indotti a prestare inconsapevolmente il consenso all'installazione di cookie a fini pubblicitari. La Corte ha chiarito che un

[191] G. BIANCARDI, *Il trattamento dei dati personali nel prisma dell'ingiustificato arricchimento*, in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2024, 641-667.
[192] Corte giust. (Grande Sezione), 1° ottobre 2019, causa C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:246.

simile meccanismo non configura un consenso valido: l'utente non può considerarsi consenziente se deve intervenire attivamente solo per negare l'autorizzazione al trattamento dei propri dati, poiché manca una manifestazione libera e consapevole della volontà[193]. Il consenso, tuttavia, si presenta come un sistema piuttosto ambiguo: da una parte incarna il potere di autodeterminazione del soggetto, dall'altra degrada a mero presupposto di liceità del trattamento. Il dibattito attuale è tra due scuole di pensiero: coloro che riconoscono al consenso una funzione 'autorizzatoria' dal valore integrativo, al fine di rendere concretamente esercitabili attività lecite interdette da limiti posti a protezione dell'interessato, e coloro che non escludono che il consenso al trattamento possa divenire una prestazione contrattuale[194].

Un caso che ha contribuito all'accensione del dibattito sul tema è rappresentato dalla decisione del 29 novembre 2018 dell'Autorità garante della concorrenza e del mercato di adottare un provvedimento sanzionatorio nei confronti di Facebook Inc, e Facebook Ireland Ltd. La modifica delle condizioni d'uso di *WhatsApp* a seguito dell'acquisizione del controllo da parte di *Facebook* è stata oggetto di attenzione da parte dell'AGCM, che nell'ordinamento italiano tutela sia la concorrenza sia i consumatori, in applicazione del *Codice del consumo*. Con un primo provvedimento, nel maggio 2017, l'AGCM ha irrogato a *WhatsApp* una sanzione di 3 milioni di euro per una pratica commerciale scorretta di tipo aggressivo ai sensi degli artt. 20, 24 e 25 del *Codice del consumo*, concernente la modifica delle condizioni generali di contratto. Secondo gli accertamenti dell'Autorità, nell'agosto 2016 *WhatsApp* avrebbe indotto i propri utenti ad accettare integralmente le modifiche apportate ai termini di utilizzo dell'applicazione

[193] G. GUERRA, *L'impatto dei dark patterns sul consenso dell'utente: la via europea per affrontare le nuove vulnerabilità*, in *Giustizia Civile.com*, 8, 2022, 1-48.
[194] A. ALPINI, *I vizi del consenso fra contratto e trattamento dei dati: la riconoscibilità dell'errore*, in *Persona e Mercato*, 2022, 205-215.

WhatsApp Messenger, preimpostando l'opzione che consente la condivisione con *Facebook* di alcuni dati personali a fini di profilazione commerciale e pubblicitari. In caso di mancata accettazione, sarebbe stata prospettata l'interruzione del servizio[195]. In seguito, l'Autorità ha respinto le argomentazioni del social network tese a escludere l'applicazione del Codice del consumo sulla base della gratuità dei servizi offerti. Sebbene tale gratuità sia effettiva, essa rappresenta un corrispettivo per l'utilizzo pubblicitario dei dati personali degli utenti. Di conseguenza, l'accesso alla piattaforma configura un rapporto contrattuale a titolo oneroso, in quanto l'assenza di un corrispettivo monetario è compensata dallo sfruttamento economico delle informazioni personali degli utenti. Pertanto, le condizioni generali di utilizzo del servizio rientrano nell'ambito di applicazione del Codice del consumo. L'AGCM ha rilevato che gli utenti del social network non sono stati adeguatamente informati circa l'utilizzo dei loro dati personali, in quanto la gratuità del servizio viene enfatizzata a scapito della trasparenza sulle finalità commerciali. Inoltre, l'Autorità ha rilevato la natura aggressiva delle pratiche adottate da Facebook, che cede i dati degli utenti a società partner senza un'adeguata informativa né il previo consenso esplicito degli interessati. L'AGCM ha altresì evidenziato come le condizioni generali di utilizzo limitino significativamente la libertà degli utenti nella configurazione delle proprie pagine personali, subordinando l'accesso a determinate funzionalità alla condivisione dei dati personali.

Alla luce di tali violazioni, l'Autorità ha ritenuto fondate le sanzioni irrogate nei confronti della società. In un comunicato ufficiale, ha inoltre ribadito la necessità che i social network garantiscano la chiara identificazione dei contenuti pubblicitari, al fine di evitare che questi vengano

[195] S. GOBBATO, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *Media Laws*, 2019, 148-161.

confusi con altre tipologie di informazioni[196]. La decisione è stata però impugnata dinanzi al Tribunale Amministrativo Regionale (di seguito, TAR) del Lazio da Facebook Ireland e Facebook Inc., adducendo, tra gli altri motivi, l'assoluta carenza di attribuzione da parte dell'AGCM, in quanto: (a) in assenza di un corrispettivo pecuniario, non si configurerebbe una pratica commerciale e (b) la disciplina applicabile dovrebbe essere esclusivamente quella in materia di privacy, in virtù del principio di specialità sancito dall'art. 3(4) della Direttiva sulle pratiche commerciali sleali[197]. Il Consiglio di Stato[198], confermando la decisione di primo grado, ha rilevato l'assenza di incompatibilità o antinomia tra la normativa sulla protezione dei dati personali e quella sulla tutela del consumatore. Le due discipline risultano, invece, complementari, ciascuna imponendo specifici obblighi informativi volti, rispettivamente, a garantire la protezione dei dati personali e del loro trattamento, nonché a promuovere la consapevolezza delle scelte economiche del consumatore. Se i diritti relativi alla privacy sono fondamentali e inviolabili, ogni rinuncia ad essi da parte degli interessati risulterebbe nulla, poiché questi non saranno mai espropriabili dall'interessato, nemmeno su sua volontà. A seguito della sentenza emessa dal Consiglio di Stato, *Facebook* ha adottato alcune misure volte a porre fine all'infrazione. In particolare, ha modificato il messaggio sulla pagina di iscrizione "è gratis e lo sarà per sempre" con la dicitura "è veloce e facile" e ha inserito nella pagina di iscrizione un collegamento ipertestuale alle *Condizioni d'uso* e alla normativa sui dati personali. Tali misure, tuttavia, non sono state ritenute sufficienti dall'Autorità Garante della Concorrenza e del Mercato (AGCM), poiché

[196] P. MOURON, *Les conditions générales d'utilisation de Facebook sont soumises au Code de la consommation selon l'autorité de la concurrence italienne*, in *Revue européenne des médias et du numérique*, 49, 2019, 19-21.
[197] S. M. LENER, *Personal data as counter-performance in exchange for contents or services after amendments to the Italian Consumer Code*, in *Rivista di Diritto Privato*, 1, 2024, 135-154.
[198] A. SOLA, *Ambiti di interesse per la regolazione delle economie dei dati nel rapporto tra diritto e tecnologia*, in *Federalismi.it*, 10, 2023, 195-217.

continuava a mancare un'informazione immediata e chiara sull'utilizzo dei dati raccolti e sul valore economico di questi ultimi. In altri termini, risultavano ancora assenti indicazioni trasparenti sul "prezzo" effettivo del servizio, che – non potendo considerarsi un'informazione accessoria – avrebbe dovuto essere resa evidente, e non relegata in un link accanto al pulsante d'iscrizione. Per tali motivi, con provvedimento del 9 febbraio 2021 (n. 28562), l'AGCM ha irrogato a *Facebook Ireland* due nuove sanzioni, per un ammontare complessivo di sette milioni di euro[199].

Un tema di grande attualità riguarda la possibilità, introdotta dal Data Governance Act (DGA), di esprimere consenso all'altruismo dei dati, ovvero alla cessione volontaria dei propri dati personali per finalità solidaristiche. Tale meccanismo è promosso dal DGA al fine di incentivare l'uso dei dati nell'interesse collettivo, concependoli come un bene comune. Tuttavia, questo solleva rilevanti interrogativi in merito al principio del consenso specifico: in tali circostanze, infatti, l'interessato non è in grado di conoscere con precisione, al momento della prestazione del consenso, le modalità e gli scopi futuri del trattamento dei dati, rendendo difficile una vera informazione preventiva. Una problematica analoga si riscontra nel trattamento automatizzato dei dati personali: spesso l'utente acconsente a un trattamento iniziale che risulta difficilmente definibile a priori, sia in termini tecnici che giuridici, e la cui comprensione risulta particolarmente ardua anche a causa della complessità dei sistemi algoritmici coinvolti[200].

[199] F. BATTAGLIA, *La raccolta di dati da parte di Meta Platforms tra tutela dei dati personali, diritto della concorrenza e protezione dei consumatori*, in *Ordine internazionale e diritti umani*, 2022, 1048-1058.
[200] P. STANZIONE, *Introduzione*, in *Libertà e liceità del consenso nel trattamento dei dati personali*, a cura di S. ORLANDO, Firenze, Persona e Mercato ed., 2024, 5-7.

2.4 Proprietà, controllo e uso dei dati: modelli normativi a confronto

In passato, le decisioni politiche e normative si basavano su dati storici e statistiche. Quest'ultimo termine implica una certa staticità, come suggerisce l'etimologia della parola stessa (statistica). Oggi, invece, grazie all'avanzamento delle tecnologie, in particolare quelle legate all'Internet delle cose, i dati vengono raccolti, elaborati e analizzati in tempo reale. Questo cambiamento comporta la possibilità di prendere decisioni, anche in ambito giuridico, in maniera immediata, come nel caso di misure urgenti quali la chiusura di una strada a seguito di un incidente o il blocco dell'importazione di un prodotto per motivi sanitari[201].

Nella società tecnologica globalizzata, i dati personali sono stati descritti come *global commons*: un patrimonio accessibile a molti, ma al tempo stesso fragile e prezioso, poiché strettamente legato all'essenza dell'individuo. Il diritto alla protezione dei dati personali rappresenta una declinazione specifica del più ampio diritto alla privacy, che oggi si rivela fondamentale per tutelare la libertà e la dignità della persona[202].

I sostenitori del liberismo sono tuttavia convinti che la commercializzazione delle informazioni personali porti vantaggi non solo alle aziende ma anche ai consumatori: per le aziende, poiché grazie alla profilazione possono soddisfare meglio le preferenze dei clienti e stimolare lo sviluppo tecnologico e l'innovazione per offrire prodotti migliorati; per i consumatori, perché hanno accesso a una gamma più ampia e diversificata di prodotti e servizi più adatti alle loro esigenze.

---

[201] V. ZENO-ZENCOVICH, *Big data e epistemologia giuridica*, in *Governance of/through Big Data*, a cura di G. RESTA, Roma, Roma Tre Press, 2023, 439-440.
[202] A.G. PARISI. *Il regolamento generale sulla tutela dei dati personali. Responsabilità e sanzioni*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G. M. RICCIO, Padova, CEDAM, 2016, 289-311.

La vera questione riguarda però il modo in cui tali informazioni vengono raccolte: da qui deriva la necessità di stabilire regole di controllo per prevenire eventuali illeciti da parte delle imprese, dato che la compensazione dei danni appare inefficace in quanto spesso interviene troppo tardi, ossia dopo che il danno si è già verificato. Allo stesso tempo emerge una presunta contraddizione: l'individuo possiede un'identità digitale con cui si riconosce o viene identificato, ma proprio per questo non dovrebbe esserne il proprietario; al contrario, soggetti terzi possono appropriarsene e vantare diritti di proprietà su di essa. Infatti, la normativa (anche a livello europeo) che regola le banche dati tutela la proprietà di chi ha raccolto dati altrui. Questa apparente contraddizione non è però definitiva: i dati riconducibili a una persona sono migliaia, e selezionarli per raccoglierli, organizzarli, configurarli richiede un'attività complessa che comporta un costo, e perciò è giusto che chi abbia svolto questo lavoro venga adeguatamente compensato. Diverso è invece il caso della persona "che si appropria di sé stessa": questo rappresenta un dilemma su cui la dottrina discute e si interroga fin dai tempi della nascita del diritto generale della personalità, ma la scelta europea fu quella di non considerare l'individuo come oggetto di proprietà di sé stesso[203]. L'informazione, a causa della sua composizione naturale si riconduce al *genus* delle *res incorporales*, in quanto sprovvista sia di forma che di struttura. Quest'ultima, tuttavia, si concretizza e si tramuta in oggetto capace di catturare l'attenzione del diritto ad alcune condizioni: nel momento in cui viene fissata o registrata su di un supporto che va ad attribuirle in tal modo il requisito della corporalità od anche nel momento in cui viene comunicata all'esterno, cioè pubblicata. Il processo di digitalizzazione stesso consente, in una certa misura, che l'informazione (se concepita in senso lato), da entità eterea, acquisti una sua consistenza proprio grazie a quel processo di

[203] G. ALPA, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. ZORZI GALGANO, Milano, Cedam - Wolters Kluwer, 2021, 11-32.

trasformazione del dato in linguaggio leggibile dalle macchine che le permette di rimanere iscritta nella memoria, temporanea o duratura che sia, dell'elaboratore elettronico di riferimento[204].

I dati rappresentano un *quid* tanto rilevante per le imprese e le istituzioni contemporanee quanto estremamente difficile da inquadrare sotto il profilo giuridico. La domanda che si pone, dunque, è: cosa sono i dati? Questo quesito è chiaramente centrale per stabilire il regime di circolazione e di accesso, ma risulta complesso trovare una risposta facendo riferimento alle categorie giuridiche tradizionali[205]. S. Orlando[206] invita a riflettere criticamente sull'etimologia della parola "dato". Per *dato* tradizionalmente si fa riferimento ad un'informazione oggettiva, un elemento a nostra conoscenza e di cui abbiamo la disponibilità all'utilizzo. Solitamente, infatti, consideriamo il dato come l'unità fondamentale della conoscenza. Tuttavia, sarebbe più corretto riferirsi ad esso come a un *captum*, cioè a ciò che l'essere umano riesce a percepire e afferrare della realtà. Anche N. Irti[207] critica l'idea di oggettività suggerita dalla parola 'dato' ed utilizza a tal fine la contrapposizione tra 'dato' e 'costruito' (*donnée* vs *construit*). Questa riflessione teorica diventa particolarmente rilevante se consideriamo la crescente datificazione del mondo: come evidenziato da E. Calzolaio, esistono diverse tipologie di dati, tra cui i dati derivanti dalla conversione degli oggetti del mondo reale in dati digitali, i dati relativi alla datificazione delle informazioni (notizie, risultati di ricerche, ecc.), i dati personali, acquisiti attraverso piattaforme e servizi online, che permettono di ottenere informazioni su aspetti sensibili come età, nome, comportamento, opinioni.

---

[204] P. SAMMARCO, *Diritto digitale*, Giuffrè Francis Lefebvre, 2024, 1-4.
[205] E. CALZOLAIO, *Beni digitali e proprietà tra civil law e common law*, in *Rivista Critica del Diritto Privato*, Napoli, Jovene, 2023, 3, 287-326.
[206] S. ORLANDO, *Data vs capta: intorno alla definizione di dati*, in *Nuovo Diritto Civile*, 7(4), 2022, 4, 14-53.
[207] N. IRTI, *Il tessitore di Goethe (per la decisione robotica)*, in *Decisione robotica*, a cura di A. CARLEO, Bologna, Il Mulino, 2019, 17-31.

Nel mondo dell'informatica, invece, i dati sono principalmente definiti in base alla loro utilità per i computer. Secondo il Vocabolario della Tecnologia dell'Informazione dell'ISO/IEC[208], i dati sono una "*rappresentazione reinterpretabile delle informazioni in modo formalizzato, adatta per la comunicazione, l'interpretazione o l'elaborazione*". Un'altra definizione, proposta da H. Zech[209], afferma che "*i dati possono essere definiti come informazioni codificate leggibili dalle macchine*". In questo contesto, i dati sono visti come elementi o oggetti il cui scopo è consentire alle macchine di eseguire funzioni computazionali: i dati rendono utili i computer[210].

Inizialmente, il trattamento dei dati personali era considerato un'attività accessoria rispetto all'oggetto e alla finalità del contratto. Ciononostante, come descritto, negli ultimi anni si sono ampiamente diffusi modelli contrattuali in cui la cessione dei dati personali dell'interessato è utilizzata come forma di compenso per l'accesso a contenuti o servizi digitali. Ad oggi, non è più solo il sistema dei media tradizionali a minacciare il diritto alla riservatezza, ma soprattutto l'uso pervasivo e invisibile dei dati personali da parte di operatori economici e altre entità. La riflessione dottrinale, vasta e articolata, ha portato alcuni a proporre l'estensione del regime di proprietà[211] anche ai dati. In particolare, la dottrina tedesca, seguendo il modello di illecito

---

[208] ISO/IEC, *Information technology — Vocabulary (ISO/IEC 2382:2015)*, 2015.
[209] H. ZECH, *Data as a tradeable commodity*, in A. DE FRANCESCHI (ed.), *European contract law and the digital single market: Implications of the digital revolution*, Cambridge, Intersentia, 2016, 51-80.
[210] I. STEPANOV, *Introducing a property right over data in the EU: the data producer's right – an evaluation*, in *International Review of Law, Computers & Technology*, 34(1), 2019, 65-86.
[211] I diritti di proprietà sono stati oggetto di discussione, analisi e tentativi di definizione nel corso dei secoli. Non esiste un concetto univoco di proprietà. Storicamente, derivando dal diritto romano, i diritti di proprietà erano principalmente associati a beni materiali, cioè a beni tangibili. Tuttavia, il concetto classico di diritti di proprietà tangibili non corrisponde completamente alla realtà contemporanea. Di conseguenza, è emersa un dibattito sull'adattamento dei diritti di proprietà alle nuove realtà, estendendo la loro applicazione dai beni materiali a quelli immateriali. È in questo contesto che la teoria della proprietà si è sviluppata negli ultimi due secoli. Pertanto, brevetti, diritti d'autore e marchi, tutti a protezione di beni immateriali di valore, sono oggi considerati diritti di proprietà.

civile del BGB[212], si è posta la questione relativa ai dati, i quali potrebbero essere oggetto di un diritto di proprietà per garantire una tutela adeguata in caso di danni, come la distruzione dei dati causata da virus[213].

Il termine "bene informatico" fu utilizzato per la prima volta in Italia negli anni '80 del Novecento per indicare dati, informazioni e software presenti all'interno di dispositivi informatici. A lungo dottrina e giurisprudenza si sono interrogate sull'eventuale assimilabilità di tali beni, ai fini della tutela penale, ai beni di natura materiale. Il dubbio emergeva soprattutto in riferimento a fattispecie di reato come il furto o il danneggiamento. Tuttavia, la risposta fu prevalentemente negativa, in quanto non è possibile qualificare come "beni corporali" elementi privi di tangibilità. La proprietà, infatti, si applica a beni aventi consistenza fisica, rendendo inapplicabile tale concetto ai cosiddetti beni informatici.

La necessità di tutelare, regolamentare e soprattutto disciplinare il bene informatico deriva dall'incessante evoluzione delle reti digitali e dalla diffusione capillare dei dispositivi elettronici mobili. Questo sviluppo ha determinato una crescente esposizione dei sistemi a rischi e vulnerabilità, generando una duplice esigenza: da un lato, l'introduzione di un corpus normativo che protegga e disciplini il bene giuridico in questione; dall'altro, l'adozione di misure di sicurezza idonee a garantire un controllo efficace, incentivando al contempo l'uso dei sistemi digitali e promuovendo una sempre più ampia "libera circolazione delle informazioni[214]".

---

[212] Il *Bürgerliches Gesetzbuch* (comunemente indicato con le iniziali BGB) è il codice civile della Germania.

[213] Di seguito viene riportato in lingua inglese il testo della sezione 823 del BGB: "*Liability in damages (1) A person who, intentionally or negligently, unlawfully injures the life, body, health, freedom, property or another right of another person is liable to make compensation to the other party for the damage arising from this. (2) The same duty is held by a person who commits a breach of a statute that is intended to protect another person. If, according to the contents of the statute, it may also be breached without fault, then liability to compensation only exists in the case of fault."*

[214] V. S. Z. B. PEPOLI, *Profili di contrasto al cybercrime in iure condito e de iure condendo*, in *Rivista Italiana di Informatica e Diritto*, 4(2), 2022, 109-121.

I dati, a differenza degli altri beni, possono essere utilizzati da molti soggetti senza esaurirsi o deteriorarsi. Il loro valore non risiede nel singolo dato, ma nella loro aggregazione ed elaborazione tramite strumenti informatici.

Nel sistema giuridico europeo è indubbio che i dati personali siano oggetto di protezione all'interno dei Trattati, ma il fatto che un diritto venga qualificato come fondamentale implica in maniera necessaria che il soggetto non possa disporne? I diritti fondamentali sono riconducibili a due paradigmi di fondo che trascendono il diritto e si arricchiscono di concezioni antropologiche e filosofiche ben radicate all'interno della società. Nel primo, liberale e di matrice soggettivistica, i diritti sono liberamente disponibili e rinunciabili. Nel secondo, dignitario e di matrice oggettivistica, i diritti sono un *datum* originale, indivisibili dall'uomo stesso. Questi due sistemi, ovviamente, nel dibattito giuridico contraddistinto dalla ragion pratica e non dalla ragion pura si contaminano fra loro a seconda delle casistiche. Nell'attuale periodo storico, il fatto che un diritto venga qualificato come fondamentale non significa escludere, in maniera assoluta, la disponibilità da parte del soggetto, sebbene vi siano forti eccezioni derivate dal paradigma dignitario. Il fatto che un diritto sia disponibile non implica di per sé che esso sia anche commerciabile. In alcuni casi troviamo una forma di indisponibilità definibile come "relativa", per cui la commerciabilità non è implicabile, come per ciò che concerne il divieto di maternità surrogata (il cosiddetto utero in affitto). Ciò è dovuto alla natura del nostro sistema giuridico che, per ossequiare al principio di eguaglianza, deve garantire delle tutele particolari nei settori in cui si vengono a porre delle relazioni giuridiche tra soggetti che non sono sullo stesso piano sociale, economico, cognitivo o psicologico. Il principio di indisponibilità, quindi, esprime l'interesse del sistema costituzionale di rimuovere, a livello fattuale, squilibri nei rapporti contrattuali che porterebbero la parte più debole ad acconsentire a condizioni

ingiustificate o sfavorevoli. L'ulteriore questione che si pone è relativa ai dati personali, se oltre che disponibili, questi siano anche commerciabili[215].

Il mercato dei dati negli Stati Uniti, al contrario di quello dell'Unione, ha conosciuto una rapida espansione, favorito da un approccio liberale e da un quadro giuridico in materia di dati non ancora ben definito. In particolare, si distingue una controversia tra due visioni principali riguardo ai diritti sui dati. Una prospettiva, come descrive E. Calzolaio[216], sostiene che i dati possono essere considerati oggetto di diritti di proprietà qualora il titolare eserciti un controllo effettivo su di essi, che include la facoltà di accesso, utilizzo, modifica e concessione di diritti ad altri. In questa ottica, il controllo su almeno una copia dei dati conferirebbe diritti di proprietà. Al contrario, un'altra visione afferma che solo gli oggetti sui quali si possa esercitare un dominio assoluto possono essere considerati appropriabili, escludendo quindi i dati dalla logica proprietaria tradizionale. In linea con la retorica del marketplace e del free speech, negli Stati Uniti vige – almeno sul piano dichiarativo – un principio generale di libera circolazione dei dati, che impone restrizioni rigorose alle limitazioni che potrebbero ostacolarne o indebitamente restringerne il flusso.

La protezione dei dati non gode di un riconoscimento costituzionale e non esiste una normativa federale unitaria sulla privacy, la cui regolamentazione è demandata alle singole legislazioni statali. Anche laddove presenti, tali normative sono principalmente finalizzate a garantire il corretto funzionamento del mercato.

---

[215] A. SIMONCINI, *Do ut Data: quali limiti costituzionali alla cessione dei dati personali?*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024.
[216] E. CALZOLAIO, *Beni digitali e proprietà tra civil law e common law*, in *Rivista Critica del Diritto Privato*, Napoli, Jovene, 2023, 3, 287-326.

Gli eventuali abusi nell'uso dei dati vengono sanzionati solo qualora abbiano determinato un danno concreto al consumatore e siano riconducibili a pratiche commerciali scorrette o a una carenza di trasparenza informativa[217].

Non vi è dubbio quindi che, al contrario di quanto descritto per il sistema europeo, negli Stati Uniti i dati siano trattati come liberamente appropriabili, anche nel caso in cui si trattino dati personali, e che ciò abbia permesso una notevole crescita delle imprese del settore con minimi vincoli e costi contenuti. Si ricorda che le prime riflessioni economiche sulla privacy negli Stati Uniti si concentravano soprattutto sull'efficienza dei mercati delle informazioni personali. Poiché il Privacy Act del 1974 regolava esclusivamente i registri pubblici, la questione principale riguardava se anche la raccolta e l'utilizzo delle informazioni personali da parte di soggetti privati dovessero essere soggetti a vincoli normativi. La Chicago School sosteneva che la regolamentazione era superflua, ritenendo che i mercati delle informazioni personali potessero funzionare con la stessa efficienza dei mercati tradizionali di beni e servizi. Ciononostante, tale impostazione trascurava le modalità concrete con cui le informazioni personali vengono raccolte. Dati accurati non sorgono spontaneamente: raccoglierli richiede risorse, e tale attività può produrre effetti indesiderati sul benessere dei consumatori. Inoltre, la Chicago School si concentrava quasi esclusivamente su una dimensione della privacy, la segretezza, trascurando altre due componenti altrettanto essenziali: autonomia e riservatezza[218].

In contrapposizione, in Europa non esistono grandi società nel settore dei dati, dal decennio degli anni '80 fino al GDPR del 2016, la protezione dei dati personali è stata elevata a diritto fondamentale, rientrante tra i diritti della personalità (nome, reputazione, immagine), attribuendo ai titolari dei dati il

[217] G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE Online*, 57(1), 2023, 339-369.
[218] K.-L. HUI e I. P. L. PNG, *The economics of privacy*, in T. HENDERSHOTT (ed.), *Handbooks in Information Systems: Volume 1: Economics and Information Systems*, Elsevier, 2006.

potere di esigere il rispetto delle norme e dei principi stabiliti per il loro trattamento da parte di terzi[219]. Sebbene l'idea di un GDPR statunitense possa apparire teoricamente affascinante, W. Hartzog e N. M. Richards[220] ritengono che una simile legislazione risulterebbe sostanzialmente inadeguata se applicata. La principale motivazione di tale conclusione risiede nelle divergenze fondamentali tra i diritti alla privacy negli Stati Uniti e quelli riconosciuti nell'Unione Europea. Negli Stati Uniti, tali diritti tenderebbero a configurarsi come diritti di protezione dei consumatori, orientati verso la salvaguardia degli interessi economici, e sarebbero suscettibili di essere limitati nel corso del processo legislativo a causa delle pressioni esercitate dai gruppi di lobby delle imprese tecnologiche. In netto contrasto, il GDPR si fonda su un solido ancoraggio costituzionale di diritti fondamentali alla privacy, che non trovano equivalente nel diritto statunitense vigente. L'Unione Europea ha storicamente tutelato la privacy come un diritto costituzionale esplicito, con due diritti fondamentali distinti: il diritto al "rispetto della vita privata e familiare" (Articolo 7) e il diritto alla "protezione dei dati personali" (Articolo 8)[221]. Inoltre, tali diritti europei sono soggetti alla dottrina dell'"*horizontal effect*", che impone agli Stati membri di garantire adeguatamente i diritti fondamentali anche contro le violazioni perpetrate da altri soggetti della società. Pertanto, le garanzie sancite dal GDPR trascendono la mera regolamentazione commerciale: in quanto attuazione diretta ed estensione dei diritti costituzionali, il GDPR deve essere inteso come dotato di uno status costituzionale. L'attuale modello del diritto sulla privacy negli Stati Uniti si basa invece sul principio di "*notice and choice*," secondo il quale le imprese sono soggette a tre regole principali: (i) non

[219] E. CALZOLAIO, *Beni digitali e proprietà tra civil law e common law*, in *Rivista Critica del Diritto Privato*, Napoli, Jovene, 2023, 3, 287-326.
[220] W. HARTZOG e N. M. RICHARDS, *The surprising virtues of data loyalty*, in *71 Emory Law Journal*, 2022, 985-1033.
[221] Consiglio d'Europa. (1950). Convenzione per la protezione dei diritti dell'uomo e delle libertà fondamentali, art. 7-8, 4 novembre 1950

mentire sulle proprie pratiche relative ai dati, (ii) non causare danni irragionevoli (i danni ragionevoli sono considerati accettabili), e (iii) rispettare le *Fair Information Practices*[222], in particolare il citato principio di "*notice and choice*". In pratica, queste regole permettono alle aziende di fare sostanzialmente ciò che desiderano con i dati delle persone, a patto che abbiano mostrato una vaga informativa sulla privacy, non causino danni economici o danni significativi di altro tipo e non mentano su quanto stiano facendo nelle loro informative sulla privacy. Consci delle poche garanzie che presenta il sistema americano, W. Hartzog e N. M. Richards propongono una soluzione basata sull'applicazione del principio di lealtà (*loyalty*), che trasformerebbe significativamente l'attuale quadro normativo. Tale principio imporrebbe alle aziende un obbligo vincolante di agire nell'interesse dei propri clienti, impedendo loro di giustificare pratiche di trattamento dei dati finalizzate principalmente ai propri fini, spesso celate dietro termini e condizioni vaghi nelle informative sulla privacy. In questo modo, gli utenti, nel prendere decisioni, avrebbero la garanzia che le opzioni proposte non comportino manipolazioni da parte delle aziende.

La possibilità di scambiare dati personali in cambio di prodotti, servizi o altri incentivi (cioè, i dati personali come controprestazione in un accordo) dipende dall'approccio adottato rispetto al diritto alla protezione dei dati. In Europa, come più volte affermato, tale diritto è riconosciuto come un diritto fondamentale e come un diritto della personalità. Ne deriva una tensione tra, da un lato, la protezione dei dati personali come elementi immateriali dell'identità individuale – la nostra "anima digitale" – che porta a sostenere l'inalienabilità dei dati personali, e, dall'altro, il loro sfruttamento

[222] Su queste tematiche sono pertinenti gli studi: N. M. RICHARDS e W. HARTZOG, *Taking trust seriously in privacy law*, in *Stanford Technology Law Review*, 19, 2017; W. HARTZOG, *Privacy's blueprint: The battle to control the design of new technologies*, Harvard University Press, 2018; W. HARTZOG e N. M. RICHARDS, *Privacy's constitutional moment and the limits of data protection*, in *Boston College Law Review*, 58(6), 2015; D. J. SOLOVE, *Introduction: Privacy self-management and the consent dilemma*, in *Harvard Law Review*, 126(7), 2013.

in chiave economica[223]. Ciò che si intende sottolineare, in altre parole, è il pericolo che un disallineamento normativo possa tradursi, in un ambito così strettamente connesso alle capacità di investimento di Stati e imprese, anche in un'alterazione degli equilibri di mercato: da un lato, "favorendo" quegli ordinamenti meno stringenti che offrono maggiore flessibilità normativa e prospettano rendimenti più elevati per gli investimenti; dall'altro, "penalizzando" gli ordinamenti degli Stati membri soggetti a vincoli più severi.

Si tratterebbe di una dinamica simile a quella che ha interessato i fornitori di servizi digitali, e in particolare le grandi piattaforme, che hanno potuto prosperare in contesti normativi più permissivi – come quello statunitense – caratterizzati da una minore presenza di vincoli regolatori e da una visione che interpreta la loro affermazione come un mezzo per potenziare la *freedom of speech*, considerata un principio fondante di quell'ordinamento[224].

In sintesi, il timore è che un livello inferiore di protezione del diritto alla riservatezza, negli ordinamenti meno attenti a tale valore, possa tradursi in un vantaggio competitivo ottenuto, in definitiva, a scapito dei diritti degli individui.

2.5 Il diritto alla portabilità dei dati tra *datification* e *data protection by design*

Il diritto di accesso e il diritto alla portabilità dei dati rappresentano strumenti particolarmente efficaci di tutela individuale, capaci di rafforzare il controllo dell'interessato sulle proprie informazioni personali senza, tuttavia, ostacolare la concorrenza o comprimere – almeno potenzialmente – la libera

[223] M. MURSIA e C. A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in *Media Laws*, 2, 2021, 165-189.
[224] M. BASSINI, *Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica*, in *Diritto Costituzionale*, 2023, 1, 83-112.

circolazione dei dati. Nell'ambito delle diverse soluzioni interpretative emerse a livello internazionale, il modello europeo si distingue per il rifiuto della prospettiva liberale che mira a qualificare i dati personali come nuove forme di proprietà ("*new properties*"), preferendo invece una logica improntata al bilanciamento tra diritti fondamentali, autonomia informativa e interesse pubblico[225]. Il diritto alla portabilità dei dati personali è stato introdotto dall'art. 20 del Regolamento Generale sulla Protezione dei Dati (GDPR) ed è considerato una delle novità più rilevanti del regolamento, rappresentando un elemento chiave del modello europeo di regolazione dell'economia digitale. La polivalenza del diritto alla portabilità si riflette nella pluralità delle finalità che lo sorreggono: accanto alla sua funzione essenziale di riequilibrio nei rapporti tra titolare del trattamento e interessato, volta a rafforzare il controllo individuale sui dati personali, sono emerse anche ricadute positive di più ampio respiro, che investono l'intera platea dei consumatori e, in generale, gli utenti dei servizi digitali[226].

Già nella Comunicazione sull'economia dei dati del 2014, la Commissione Europea aveva evidenziato l'importanza della portabilità dei dati per la costruzione di un mercato interno dei dati, ma è negli ultimi anni che tale strategia si è meglio definita. La Commissione ha tradotto questa visione in iniziative strettamente interconnesse, volte a promuovere la libera circolazione dei dati come quinta libertà fondamentale dell'Unione Europea[227]. Negli ultimi anni, la Commissione ha ulteriormente precisato e concretizzato attraverso iniziative interconnesse e complementari la Strategia Europea sui dati e la libera circolazione dei dati. La nozione sottostante è

---

[225] G. PIGNATARO, *Circolazione dei dati tra modelli proprietari e contrattuali*, in *Media Laws*, 2, 2024, 1-26.
[226] S. GATTI, *Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati*, in *European Data Law. European Journal of Privacy Law & Technologies*, 1, 2024, 158-177.
[227] E. BANI e E. MACCHIAVELLO, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, in *Financial Innovation tra disintermediazione e mercato*, a cura di V. FALCE, Torino, Giappichelli, 2015, 137-179.

semplice: consentire a ogni individuo che utilizza servizi online di trasferire i propri dati personali da un servizio/fornitore all'altro, garantendo il pieno riutilizzo autonomo senza perdere il patrimonio informativo accumulato in precedenza. A livello europeo, il precedente logico e storico è rappresentato dalla portabilità del numero telefonico tra operatori e dalla portabilità dei mutui. In tutti questi contesti, uno dei principali motivi per il diritto alla portabilità è quello di promuovere la concorrenza tra gli operatori a vantaggio degli utenti, con effetti regolatori significativi sui mercati digitali[228].

Il diritto alla portabilità impone precise responsabilità agli operatori dei mercati digitali, estendendosi oltre i diritti individuali. Esso esercita un'influenza sulla configurazione stessa del mercato, modellandone le dinamiche concorrenziali. In particolare, vi sono due effetti desiderati interconnessi che richiedono una considerazione regolativa: da un lato, la prospettiva del consumatore implica la riduzione dei costi associati al cambio di fornitore; dall'altro, dal punto di vista dell'impresa, si mira ad abbattere le barriere all'ingresso sul mercato. I costi di *switching*, cioè gli ostacoli che i consumatori devono superare quando intendono cambiare fornitore di servizi (*switch*), costituiscono un elemento chiave per il corretto funzionamento di un mercato competitivo. Quando tali costi superano i benefici che il consumatore potrebbe ottenere passando a un altro fornitore, si verifica il fenomeno del *lock-in*, situazione in cui i consumatori rimangono "vincolati" a un determinato servizio anche se esistono alternative più vantaggiose. Maggiore è l'incremento dei costi di switching, maggiore è il grado di *lock-in* dei consumatori e più difficile diventa per un nuovo operatore entrare nel mercato con un servizio concorrente[229].

[228] A. G. MONTELEONE, *Il diritto alla portabilità dei dati: tra diritti della persona e diritti del mercato*, in *LUISS Law Review*, 2017, 2, 202-213.
[229] M. BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, 20(2), 2018, 223-245.

A questo punto è necessario ricordare come il modo in cui queste tecnologie sono progettate e i processi organizzativi adottati abbiano un impatto significativo sulle dimensioni giuridiche degli individui e sui loro dati personali. Pertanto, il diritto può impiegare la tecnologia come mezzo per plasmare il suo sviluppo e promuovere nuove forme di protezione normativa. Emerge così la possibilità di un quadro in cui le norme del diritto digitale possono essere integrate direttamente nella stessa tecnologia[230]. Quello della *data protection by design* è un paradigma sempre più diffuso che si basa su concetti precedenti come il "design sensibile ai valori", "il codice come legge" (*code is law*) e le Tecnologie per il Potenziamento della Privacy (*Privacy Enhancing Technologies*). Originariamente introdotte nel 1995 e ora adottate sia nella ricerca che nelle policy, le PETs hanno guadagnato il sostegno dei *policy-makers*, soprattutto nell'Unione Europea. Queste tecnologie sono viste come complementari al quadro giuridico esistente, garantendo la protezione dei dati personali nelle reti ICT. Il concetto di "privacy by design" si sostituisce gradualmente a quello delle PETs, enfatizzando l'integrazione della privacy nei sistemi fin dalla fase di progettazione e promuovendo la sua implementazione come impostazione predefinita[231]. Le linee guida dell'EDPB[232] pongono, come obbligo principale, quello di adottare misure adeguate e garanzie idonee che consentano un'efficace applicazione dei principi della protezione dei dati, tutelando così i diritti e le libertà degli interessati sin dalla fase di progettazione e per impostazione predefinita. L'articolo 25 del GDPR specifica gli elementi, relativi sia alla progettazione che alla configurazione

[230] P. GUARDA e G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023.
[231] B.-J. KOOPS e R. E. LEENES, *Privacy regulation cannot be hardcoded: a critical comment on the "privacy by design" provision in data-protection law*, in *International Review of Law, Computers & Technology*, 28(2), 2014, 159-171.
[232] European Data Protection Board (EDPB), *Linee guida WP 250: "Protezione dei dati fin dalla progettazione e per impostazione predefinita" (Versione 2.0)*.

predefinita, che devono essere considerati. L'efficacia rappresenta il fulcro del concetto di protezione dei dati fin dalla progettazione e l'obbligo di attuare i principi in modo efficace implica che i titolari del trattamento adottino misure e garanzie adeguate alla tutela di tali principi, al fine di assicurare il rispetto dei diritti degli interessati. Ogni misura applicata deve essere in grado di raggiungere gli obiettivi stabiliti per il trattamento, così come previsti dal titolare. Da questa osservazione derivano due conseguenze. Anzitutto, ciò significa che l'articolo 25 non impone l'adozione di misure tecniche e organizzative predefinite, ma richiede piuttosto che le misure e le garanzie selezionate siano strettamente collegate alla concreta attuazione dei principi di protezione dei dati in relazione allo specifico trattamento. In quest'ottica, tali misure devono essere concepite per essere solide e resilienti, e il titolare del trattamento deve poter introdurre ulteriori misure qualora si verifichi un incremento dei rischi. L'efficacia di queste misure dipenderà, dunque, dal contesto del trattamento e dalla valutazione di determinati fattori, che devono essere considerati nella fase di definizione dei mezzi del trattamento. In secondo luogo, i titolari del trattamento devono essere in grado di dimostrare il rispetto dei principi. Lo "stato dell'arte" è un concetto dinamico, che non può essere definito in modo statico rispetto a un determinato momento, ma deve invece essere oggetto di una valutazione continua nel contesto dell'evoluzione tecnologica. Alla luce di tali progressi, un titolare del trattamento potrebbe accorgersi che una misura precedentemente idonea a garantire un livello di protezione adeguato non lo sia più.

Si ricorda che, oltre ai vantaggi economici immediati, il diritto alla portabilità dei dati ha un profondo legame con la sfera personale degli interessati. Consentendo una gestione fluida delle informazioni personali sotto il controllo diretto dell'utente, questo diritto diventa uno strumento chiave per la costruzione e l'affermazione dell'identità digitale. In un ambiente connesso e senza confini temporali o spaziali, la portabilità offre agli individui il potere di governare i propri dati, incrementando la capacità

di esercitare diritti fondamentali, come quello alla salute, e contribuendo alla creazione di sistemi di gestione più efficienti e trasparenti[233]. Come già osservato, il diritto alla portabilità si applica esclusivamente ai dati personali quando il trattamento è fondato sul consenso dell'interessato oppure su un contratto, e a condizione che avvenga tramite strumenti automatizzati. Di conseguenza, una cooperativa di dati, per poter svolgere legittimamente la propria attività di intermediazione, deve rispettare non solo quanto previsto dall'articolo 12, lettera d), del Data Governance Act (DGA), ma anche i requisiti stabiliti dall'articolo 20 del GDPR. I dati soggetti al diritto alla portabilità, come previsto dall'art. 20 del GDPR, sono esclusivamente i dati personali che riguardano l'interessato e che quest'ultimo ha fornito al titolare del trattamento. In presenza delle condizioni specificate dalla norma, tali dati devono poter essere trasferiti a un altro titolare, stabilendo così una comunicazione tra due sistemi in modo sicuro e tecnicamente idoneo affinché il sistema "destinatario" sia in grado di riceverli in un formato accessibile e interpretabile. Il titolare originario è quindi tenuto a fornire i dati personali in un formato che sia strutturato, di uso comune, leggibile da un dispositivo automatico e interoperabile, così da permetterne il riutilizzo da parte del titolare ricevente[234].

Il capo VIII del Data Act in particolare è dedicato all'interoperabilità, e l'approccio normativo adottato è volto a superare il *vendor lock-in* (o blocco da fornitore). Più precisamente è l'art 33. a indicare i requisiti tecnici essenziali in materia di interoperabilità dei dati, dei meccanismi e di quei servizi di condivisione dei dati, considerando anche gli spazi europei comuni

[233] S. GATTI, *Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati*, in *European Data Law. European Journal of Privacy Law & Technologies*, 1, 2024, 158-177.
[234] C. CHILIN, *Scambio di dati, conversione di formati e interoperabilità nella fornitura del servizio di intermediazione svolto dalle cooperative di dati*, in *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, a cura di F. BRAVO, Torino, Giappichelli, 2024, 785-800.

di dati. L'art 35. va invece ad indicare "Le specifiche di interoperabilità aperte e le norme armonizzate per l'interoperabilità dei servizi di trattamento dei dati". Il Data Act si occupa anche di *smart contract*, all'art. 36 "Requisiti essenziali relativi ai contratti intelligenti per l'esecuzione degli accordi di condivisione dei dati", riconosce nei contratti intelligenti degli strumenti per la condivisione dei dati poiché essi possono garantire l'esecuzione di accordi a ciò finalizzati, assicurando sistemi interoperabili tramite le garanzie di conformità a requisiti ritenuti essenziali[235].

2.6 "Interoperable Europe Act" e il Mercato Unico Digitale Europeo

Fin dalle sue origini, sorte dalle macerie della Seconda guerra mondiale, il progetto di integrazione europea si è sviluppato profondamente, evolvendo da un semplice mercato comune per il carbone e l'acciaio fino a delineare le basi per un Mercato Unico Digitale. Nel corso di tale processo di integrazione economica, l'Unione ha consacrato le quattro libertà fondamentali che costituiscono il nucleo del mercato interno: la libera circolazione delle merci, dei capitali, dei servizi e delle persone.

La digitalizzazione, tuttavia, ha profondamente modificato l'assetto economico per il quale tali libertà erano state originariamente pensate, rendendo necessario elaborare strategie e piani d'azione mirati per rispondere efficacemente a questo mutamento strutturale. Ci si può dunque interrogare se anche l'informazione – intesa sia come dato personale sia come dato non personale – debba beneficiare delle stesse libertà nel contesto del mercato

[235] A. MORACE PINELLI, *Riflessioni introduttive,* in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2025, 1-35.

unico, inquadrandosi tra quelle già esistenti o, eventualmente, configurandosi come una nuova libertà fondamentale[236].

Negli anni Cinquanta e Sessanta, in un contesto di forte crescita economica, il Trattato di Roma del 1957 pose le basi per la Comunità Economica Europea, introducendo il mercato comune e avviando il processo di eliminazione delle barriere doganali. Politiche come la PAC e il Fondo europeo di sviluppo regionale risposero alle profonde trasformazioni sociali e demografiche del periodo, mentre la Guerra fredda e la costruzione del Muro di Berlino nel 1961 segnarono un netto divario con l'Europa orientale. Negli anni Settanta, le crisi petrolifere e la stagflazione misero alla prova la tenuta economica della Comunità, ma il processo di integrazione proseguì.

Gli anni Ottanta inaugurarono una fase nuova: il progressivo crollo dei regimi totalitari, l'affermazione di movimenti democratici, come Solidarność in Polonia, e la nascita di iniziative simboliche di unione culturale, come il programma Erasmus del 1987, favorirono l'emergere di un'identità europea condivisa. La caduta del Muro di Berlino nel 1989 e la successiva riunificazione tedesca rafforzarono questa traiettoria. Il Trattato di Maastricht del 1992 rappresentò il vero salto di qualità, dando vita all'Unione Europea e introducendo competenze comuni in settori strategici come la politica estera, la sicurezza e la giustizia. Seguirono lo Spazio economico europeo, l'attuazione degli accordi di Schengen e l'introduzione della moneta unica, completata nel 2002 con la circolazione materiale dell'euro.

Tale ampliamento delle libertà economiche e personali rese necessario un apparato normativo più rigoroso, volto a tutelare cittadini e consumatori. L'integrazione europea, dunque, non si limitò a creare un mercato, ma

[236] A. C. PENEDO, *The Regulation of Data Spaces under the EU Data Strategy: Towards the "Act-ification" of the Fifth European Freedom for Data?*, in *European Journal of Law and Technology*, 2024, 15(1).

richiese anche la definizione di un quadro giuridico in grado di garantire equità e protezione all'interno di un contesto sempre più interconnesso[237].

Nel contesto in esame, è utile ricordare che i dati esistono da sempre e sono stati raccolti da enti pubblici e privati per secoli. Ad esempio, di questa tradizione si ritrova, nel 1807, l'istituzione dell'Ufficio statistico del Regno d'Italia, sotto la direzione dell'economista Melchiorre Gioja, che seguiva il modello napoleonico. Con lo sviluppo delle tecnologie moderne, la situazione è cambiata drasticamente. Oggi, ciò che rende diverso il panorama è la quantità enorme di dati raccolti, che cresce continuamente e in maniera esponenziale richiedendo strumenti nuovi per essere analizzati e compresi. Non ci limitiamo più a conoscere ciò che è, ma siamo ora capaci di predire ciò che potrebbe essere. Il diritto, che in passato ha avuto una funzione deontica, sta evolvendo verso un ruolo diverso: esso può diventare uno strumento che aiuti a realizzare soluzioni individuate grazie all'analisi dei dati, contenute negli algoritmi[238]. L'interoperabilità rappresenta un denominatore comune dei nuovi atti normativi dell'UE in materia di dati. La ragione è evidente: essa costituisce una condizione fondamentale per garantire un'efficace condivisione delle informazioni tanto nello spazio amministrativo dell'Unione quanto nell'economia digitale europea. Le "*standardisation organisations*" fissano spesso garanzie di interoperabilità attraverso standard tecnici[239]. Il fenomeno include la definizione stessa di

[237] L. PECCHIA, A. MACCARO, *Navigating European Healthcare Regulations Through a Historical Lens*, in *Digital Environments and Human Relations: Ethical Perspectives on AI Issues*, a cura di A. FABRIS, S. BELARDINELLI, Cham, Springer Nature Switzerland, 2024, 133-146.

[238] V. ZENO-ZENCOVICH, *Big data e epistemologia giuridica*, in *Governance of/through Big Data*, a cura di G. RESTA, Roma, Roma Tre Press, 2023, 439-440.

[239] La normazione tecnica può essere definita come quell'insieme di attività volto a produrre norme che individuano le caratteristiche tecniche, merceologiche e qualitative dei prodotti industriali da immettere sul mercato, estendendosi più recentemente anche ai sistemi e processi industriali e ai servizi. L'innovazione e lo sviluppo tecnologico sono storicamente strettamente connessi alla normazione tecnica, che funge da strumento di regolazione e standardizzazione. Fino all'età moderna, tale regolazione si caratterizzava per un approccio non sistematico; è solo a partire dalla rivoluzione industriale che si avvia quella che oggi possiamo definire l'attività di normazione nel senso moderno del termine, ossia la

interoperability, formulata nel 2017 dalla International Organization for Standardization (ISO) e dalla International Electrotechnical Commission (IEC) all'interno del loro technical standard per il cloud computing. ISO e IEC definiscono l'interoperabilità nel contesto del cloud computing come "*the ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged*." L'approccio tecnico adottato da ISO e IEC è particolarmente rilevante nel contesto dei nuovi regolamenti sui dati dell'Unione Europea, poiché il Data Act fa esplicito riferimento allo standard definito da queste organizzazioni. Nel considerando 100, il Data Act afferma che le norme armonizzate di interoperabilità dei servizi di trattamento dei dati hanno il medesimo significato delle disposizioni di cui all'allegato II del regolamento (UE) n. 1025/2012 e degli aspetti di interoperabilità definiti nella norma internazionale ISO/IEC 19941:2017. La normazione dovrebbe altresì tener conto delle esigenze delle PMI. È dunque coerente che il Data Act adotti una definizione di *interoperability* molto simile a quella prevista dallo standard tecnico ISO/IEC[240]. Lo stesso concetto di interoperabilità si riconduce a 30 anni fa, con la Direttiva 91/250/CE, in cui essa è definita come "la capacità di due o più sistemi di scambiare informazioni e di usare reciprocamente le informazioni scambiate". Il concetto di interoperabilità pertanto può essere scisso in più livelli:

- Interoperabilità base la quale consente la condivisione dei dati ma non di interpretarli;

consapevole necessità di "unificare" le norme. Questo processo ha riguardato diversi ambiti, dall'uniformazione delle unità di misura, all'armonizzazione terminologica, fino all'unificazione dimensionale dei prodotti e delle loro componenti, favorendo così maggiore certezza e interoperabilità nel mercato industriale. M. A. RIZZI, F. SERINI, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 115-136.

[240] J. P. SCHNEIDER, J. ERNY, F. ENDERLEIN, *Collaborative Governance Structures for Interoperability in the EU's new data acts*, in *European Journal of Risk Regulation*, 2025, 16(1), 24-35.

- Interoperabilità strutturale che permette l'interpretazione dei dati da parte di diversi sistemi (per esempio nel settore sanitario, in cui viene fornita una struttura);
- Interoperabilità semantica che consente a sistemi diversi di collaborare per comprendere contestualmente i dati oggetto del trattamento, eliminando le ambiguità;
- Interoperabilità organizzativa che permette lo scambio di dati che sono interpretabili da sistemi diversi andando a facilitare la governance del dato, eliminando barriere amministrative e geografiche;

Solo l'ultimo livello consentirebbe di eliminare le barriere relative al linguaggio, alla comprensione e ai mezzi di lettura del dato, rendendo competitivo il mercato europeo dei dati e raggiungendo l'obiettivo che il legislatore europeo si è posto[241].

Come indica 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*" l'interoperabilità e la qualità dei dati, al pari della loro struttura, autenticità e integrità, sono fondamentali per lo sfruttamento del valore dei dati, con un riguardo particolare nel contesto della diffusione dell'IA. In tal senso i produttori e gli utilizzatori di dati hanno individuato gravi problemi di interoperabilità che ostacolano la combinazione di dati provenienti da fonti diverse sia a livello settoriale sia, in misura ancora maggiore, a livello intersettoriale. Una possibile soluzione alla problematica individuata potrebbe consistere nell'adozione di formati e protocolli compatibili, standardizzati e condivisi, che consentano di raccogliere ed elaborare in modo coerente e interoperabile

[241] G. FONSI, *Articolo 33 - Requisiti essenziali in materia di interoperabilità dei dati, dei meccanismi e servizi di condivisione dei dati nonché degli spazi comuni europei di dati*, in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2025, 681-696.

i dati provenienti da fonti eterogenee, favorendo così l'integrazione tra diversi settori e mercati verticali. Tale obiettivo dovrebbe essere perseguito attraverso il programma continuativo di normazione delle tecnologie dell'informazione e della comunicazione (ICT) e, con riferimento ai servizi pubblici, mediante il rafforzamento del quadro europeo di interoperabilità.

La strategia dell'Unione Europea per costruire la "sovranità digitale europea" rappresenta un tentativo di riaffermare l'identità normativa e valoriale dell'Europa a livello geopolitico, in linea con le sue radici etiche e costituzionali, anche nell'ambito digitale. Il termine "sovranità digitale" è stato utilizzato dalla presidente della Commissione Ursula von der Leyen nel suo discorso sullo stato dell'Unione del 2020[242] e, da allora, è diventato centrale in numerosi documenti ufficiali dell'UE, tra cui quelli strategici e normativi, come il Digital Services Package (DSP), che include regolamenti come il DSA, il DMA, il DGA, il Data Act e l'AI Act. Prima di radicare questa definizione di sovranità digitale nel contesto dell'Unione Europea, è fondamentale chiarire il rapporto tra "sovranità" e il concetto affine ma distinto di "governance". Si assume che la sovranità digitale rappresenti l'autorità di stabilire regole volte a regolare e disciplinare le azioni, autorità che si fonda su legittimità e controllo. Ne consegue che il processo di governance digitale si concretizza nell'esercizio delle capacità rese possibili, a priori, dalla sovranità. La sovranità, dunque, identifica la capacità intrinseca di un attore di agire (una qualità che si possiede), mentre la governance si riferisce alle interazioni tra attori sovrani e alla natura stessa delle azioni svolte (un processo che si realizza)[243]. Ciò è avvenuto anche perché l'Europa ha subito profonde trasformazioni sin dal lancio del Mercato Unico, un

[242] U. VON DER LEYEN, *A Union That Strives for More: My Agenda for Europe (Political Guidelines for the Next European Commission 2019-2024)*, Commissione Europea, https://ec.europa.eu, consultato da ultimo il 22.10.2025.
[243] C. NOVELLI *et al.*, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in *European Journal of Risk Regulation*, 2025, 16(2), 566-590.

processo di cambiamento largamente attribuibile al suo stesso successo. L'integrazione è progredita significativamente in molti settori dell'economia e della società, anche se non ovunque allo stesso livello. Oggi, si stima che circa l'80% della legislazione nazionale derivi da decisioni prese a Bruxelles. Tuttavia, l'ampliamento a 27 Stati membri ha portato a un aumento della diversità e della complessità del quadro normativo europeo, ma anche delle opportunità derivanti dalle economie di scala[244].

Questa strategia segna un punto di svolta verso una rete internet regolamentata, definita come la "terza fase di internet", mirata a garantire la sicurezza, la privacy e l'autonomia digitale dell'Europa. La raccolta e l'uso dei dati rappresentano una minaccia per i diritti individuali fondamentali, poiché possono compromettere direttamente e indirettamente la resilienza e il corretto funzionamento delle istituzioni democratiche. Tuttavia, allo stesso tempo, i dati devono essere considerati un elemento fondamentale per la sicurezza nazionale. Infatti, i dati sono il motore dell'innovazione tecnologica, sia in ambito civile che militare, e sono essenziali per lo sviluppo e l'implementazione dell'intelligenza artificiale, inclusa la sua applicazione in contesti bellici[245].

La costituzione di una solida governance dei dati che protegga i dati personali pur facilitando il libero flusso dei dati non personali è tra gli obiettivi del legislatore europeo. I regolamenti dell'UE (GDPR, Data Act, Data Governance Act) vogliono creare una base di fiducia che consente a cittadini e imprese di condividere i dati in modo sicuro, stimolando il progresso senza compromettere i diritti o la privacy. La libera circolazione

---

[244] E. LETTA, *Much More Than a Market – Speed, Security, Solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens* [Report], April 2024, Notre Europe/Institut Jacques Delors, https://institutdelors.eu/en/publications/much-more-than-a-market/, consultato da ultimo il 22.10.2025.

[245] I. DE VIVO, *Sfide esistenziali e resilienze identitarie nella geopolitica informazionale: l'identikit europeo tra sovranità e costituzionalismo digitale*, in *Diritto pubblico europeo. Rassegna online*, 2024, 23(1), 168-189.

dei dati nel Mercato Unico richiede regole e standard di governance adeguati e può allo stesso tempo incentivare l'uso primario dei dati attraverso i confini, nonché l'uso secondario, come l'uso dei dati pan-europei per sviluppare servizi a valore aggiunto sia per i cittadini che per le imprese.

L'11 aprile 2024 è entrata in vigore la normativa europea determinata come "Interoperable Europe Act", ovvero il regolamento (UE) 2024/903 [246]. Tra gli obiettivi del regolamento, vi sono quelli di favorire lo scambio di dati oltre confine e accelerare la digitalizzazione del settore pubblico. Questa normativa rappresenta un elemento chiave per raggiungere gli obiettivi del decennio digitale dell'Unione Europea, tra cui la disponibilità online di tutti i principali servizi pubblici entro il 2030. L'interoperabilità, infatti, è un pilastro essenziale per il funzionamento efficace del mercato unico digitale, agevola perciò l'integrazione delle dimensioni digitali nelle politiche pubbliche, dalla giustizia alla sanità, fino ai trasporti. Il regolamento ha anche stabilito delle norme per promuovere livelli maggiori di interoperabilità non solo nel settore pubblico dell'UE ma anche a livello transfrontaliero, definendo l'interoperabilità transfrontaliera come "*la capacità dei soggetti dell'Unione e degli enti pubblici degli Stati membri di interagire tra loro a livello transfrontaliero condividendo dati, informazioni e conoscenze attraverso processi digitali in linea con i requisiti giuridici, organizzativi, semantici e tecnici relativi a tale interazione transfrontaliera*". L'obiettivo preposto non riguarda una mera circolazione dei dati ma una sostanziale condivisione degli stessi, possibile tramite l'elevazione delle funzionalità di sistemi software affiancato ad un riutilizzo consapevole di grandi quantità di informazioni. Tale obiettivo rappresenta anche una necessità per l'Unione,

[246] Commissione Europea, *Entrata in vigore della legge su un'Europa interoperabile per migliorare la connessione dei servizi pubblici per i cittadini e le imprese*, 11 aprile 2024, https://ec.europa.eu/, consultato da ultimo il 22.10.2025.

ragion per cui un cambio di rotta dal GDPR si è reso necessario, andando ad aprire la strada ad organizzazioni sia private che pubbliche[247].

Cittadini, imprese e amministrazioni pubbliche dovrebbero trarre vantaggio dal nuovo regolamento, soprattutto quando utilizzano servizi pubblici digitali interconnessi che richiedono lo scambio di dati oltre confine. Tra i principali esempi la Commissione include il riconoscimento reciproco di diplomi e qualifiche professionali, la condivisione di dati sui veicoli per garantire la sicurezza stradale, l'accesso ai dati sanitari e sociali, nonché lo scambio di informazioni in ambiti fiscali, doganali, di accreditamento per appalti pubblici, registri commerciali e patenti di guida digitali. Si stima che la normativa consentirà risparmi annuali fino a cinque miliardi di euro, secondo quanto evidenziato dalla valutazione d'impatto.

Di particolare interesse è l'introduzione delle definizioni di Govtech e Civictech all'interno del regolamento. Per Govtech[248] si intende: "*una cooperazione basata sulla tecnologia tra attori dei settori pubblico e privato a sostegno della trasformazione digitale del settore pubblico*", mentre per "Civictech[249] si intendono le "organizzazioni della società civile". Il considerando 40 del regolamento si occupa di descrivere uno degli scopi auspicabili dei sistemi di interoperabilità suggeriti, per cui, andando ad individuare esigenze e priorità condivise in materia di innovazione e concentrandosi su sforzi comuni in materia di GovTech e sperimentazione a livello transfrontaliero si aiuterebbero gli enti pubblici dell'Unione a condividere i rischi, gli insegnamenti tratti e i risultati delle misure di innovazione. Le attività qui indicate attingeranno in particolare al ricco serbatoio dell'Unione di PMI e start-up tecnologiche. Secondo la

[247] G. FONSI, *Articolo 33 - Requisiti essenziali in materia di interoperabilità dei dati, dei meccanismi e servizi di condivisione dei dati nonché degli spazi comuni europei di dati*, in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2025, 681-696.
[248] Art. 2 del regolamento (UE) 2024/903.
[249] Cons. 39 del regolamento (UE) 2024/903.

Commissione, l'esito positivo dei progetti GovTech e delle misure di innovazione guidate dall'Europa interoperabile dovrebbe contribuire a potenziare gli strumenti GovTech e le soluzioni di interoperabilità ai fini del loro riutilizzo.

Il considerando 42 del regolamento (UE) 2024/903 prevede norme che consentono l'utilizzo di dati personali raccolti per altre finalità al fine di sviluppare specifiche soluzioni di interoperabilità nell'interesse pubblico, nel contesto dello spazio di sperimentazione normativa per l'interoperabilità, conformemente all'articolo 6, paragrafo 4, del regolamento (UE) 2016/679 (GDPR) e all'articolo 5 del regolamento (UE) 2018/1725[250]**,** rispettando l'articolo 4, paragrafo 2, della direttiva (UE) 2016/680[251]. Il regolamento in questione non costituisce una base giuridica ai sensi dell'articolo 22, paragrafo 2, lettera b), del regolamento (UE) 2016/679 o dell'articolo 24, paragrafo 2, lettera b), del regolamento (UE) 2018/1725. Esso si limita a disciplinare il trattamento dei dati personali nell'ambito dello spazio di sperimentazione normativa per l'interoperabilità, mentre qualsiasi altro trattamento richiederebbe una distinta base giuridica.

Il Framework europeo per l'interoperabilità (EIF), adottato dalla Commissione Europea il 23 marzo 2017, forniva già in precedenza linee guida su come realizzare servizi pubblici digitali interoperabili. Esso include 47 raccomandazioni concrete per le amministrazioni pubbliche, mirate a migliorare la governance dell'interoperabilità, creare relazioni inter-organizzative, ottimizzare i processi di servizi digitali e garantire che la

[250] Regolamento (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*, GU L 295, 21.11.2018, 39.

[251] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

legislazione non ostacoli tali sforzi. L'EIF rientra nell'obiettivo della Commissione di creare un Mercato Unico Digitale in Europa (Digital Single Market), con il settore pubblico che gioca un ruolo fondamentale come regolatore, fornitore di servizi ed emittente di appalti, migliorando la qualità dei servizi pubblici europei e facilitando la collaborazione digitale tra le amministrazioni[252].

Il Digital Single Market si propone nel dettaglio di offrire delle garanzie per quanto concerne il settore dei dati:

- In primo luogo, la riservatezza e la protezione dei dati personali delle persone fisiche;
- In secondo luogo, la riservatezza delle comunicazioni elettroniche delle persone fisiche e giuridiche.

Si ricorda, infatti che riservatezza e protezione dei dati personali sono diritti disciplinati dagli artt. 7 e 8 della Carta UE.

Il progetto del Mercato Unico Digitale nasce con l'obiettivo di superare i residui ostacoli di natura nazionale che ancora limitano le transazioni online, inserendosi nella tradizione del mercato comune, originariamente concepito per abbattere le barriere commerciali tra gli Stati membri. Questa evoluzione ha condotto alla realizzazione del mercato interno, fondato sui principi di libera circolazione di merci, persone, servizi e capitali. In tale contesto, la strategia *Europa 2020* ha attribuito particolare rilievo all'agenda digitale, riconoscendo il ruolo centrale delle tecnologie dell'informazione e della comunicazione (TIC) per il conseguimento degli obiettivi fissati dall'Unione. Più di recente, nelle linee politiche per il periodo 2024-2029, la Presidente della Commissione ha rimarcato la funzione propulsiva del mercato unico digitale nel liberare pienamente le potenzialità del mercato unico.

[252] European Commission, *New European Interoperability Framework: Promoting seamless services and data flows for European public administrations*, Publications Office of the European Union, 2017, https://europa.eu, consultato da ultimo il 22.10.2025.

Le implicazioni di tale processo sono molteplici: il Mercato Unico Digitale favorisce un accesso più ampio e trasparente alle informazioni, contribuisce alla riduzione dei costi di transazione e promuove modelli imprenditoriali innovativi, con effetti positivi anche sul piano ambientale. L'espansione del commercio elettronico, in particolare, si traduce in benefici concreti per i consumatori, che possono godere di un'offerta più diversificata, prezzi competitivi, beni di qualità superiore e una maggiore possibilità di confronto. Parallelamente, lo sviluppo dei servizi di *e-government* rende più efficiente la gestione degli adempimenti online e facilita l'accesso a nuove opportunità professionali e imprenditoriali all'interno dello spazio europeo[253].

All'interno dei nuovi mercati facenti parte dell'ecosistema digitale beni immateriali e servizi sono dotati di nuove modalità di fruizione, in cui nuovi modelli negoziali di fruizione temporanea e caratterizzata dalla non esclusività prendono terreno rispetto al classico diritto esclusivo di proprietà.

Una tale globalizzazione del diritto apre la strada a una nuova dimensione immateriale e delocalizzata in cui le frontiere sono assenti e le reti di comunicazione elettronica sono veicolate da piattaforme digitali online, motivo per cui il Mercato Unico Digitale necessità non solo di regole tecniche ma anche regole giuridiche[254].

I cittadini e le imprese devono avere la certezza che, soprattutto quando interagiscono con le autorità pubbliche, lo facciano in un ambiente sicuro e affidabile, nel pieno rispetto delle normative pertinenti. Le amministrazioni pubbliche devono inoltre garantire la privacy dei cittadini, nonché la riservatezza, l'autenticità, l'integrità delle informazioni fornite da cittadini e imprese.

---

[253] M. U. HAUK, C. PIERDONATI, *Ubiquità del mercato unico digitale*, 16 giugno 2025, Parlamento Europeo, https://www.europarl.europa.eu/factsheets/it/sheet/43/ubiquita-del-mercato-unico-digitale, consultato da ultimo il 22.10.2025.

[254] E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019.

In conclusione, si ricorda che, attualmente, la mancanza di interoperabilità è una delle maggiori problematiche nell'odierna visione e penetrazione delle tecnologie digitali nella società. Da un punto di vista tecnologico, questa è la capacità che due o più sistemi diversi possono riuscire a comunicare tra di loro senza che avvengano impedimenti. La capacità di far lavorare insieme i dati aumenta il valore dei contenuti forniti da tutte le fonti in gioco e favorisce sia il servizio di funzionalità migliori di sistemi software, sia le esperienze d'uso per l'utente finale[255].

Come affermato, negli ultimi anni ha acquisito centralità il concetto di sovranità digitale, inteso come la capacità di uno Stato di esercitare controllo e autonomia nel cyberspazio, assicurando indipendenza tecnologica e il dominio sui dati, in particolare quelli personali.

Un'espressione concreta di questa visione è il progetto Gaia-X, finalizzato a ridurre la dipendenza dai servizi cloud extraeuropei e a costruire un ecosistema digitale aperto e affidabile, in cui i dati possano essere condivisi in modo trasparente e sicuro. L'obiettivo è rafforzare l'autodeterminazione di cittadini e imprese europee rispetto alle sfide imposte dalle tecnologie emergenti, come l'intelligenza artificiale o l'Internet of Things.

La rilevanza della sovranità digitale si è affermata progressivamente come elemento cardine dell'agenda europea, come dimostrano le dichiarazioni della Presidente della Commissione europea, Ursula von der Leyen, che ha ribadito l'urgenza di costruire un'Europa sostenibile, digitale e rispettosa dei diritti fondamentali. La sua visione si inserisce in una strategia più ampia volta alla democratizzazione dello spazio digitale e al contenimento

[255] R. BASILI, *Interoperabilità dei dati, metodologie di condivisione e prospettive: opportunità e rischi*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 33-64.

del potere delle grandi piattaforme tecnologiche, riaffermando il primato dei valori democratici all'interno dell'ecosistema digitale europeo.

CAPITOLO III
SICUREZZA E GOVERNANCE DEI DATI

Sommario: 3.1 Sicurezza dei dati e cibersicurezza – 3.2 Data Governance, definizione e funzioni – 3.3 Valutazione del rischio – 3.3.1 Valutazione del rischio – 3.3.2 Gli strumenti di valutazione del rischio – 3.4 Valutazione di impatto (Data Protection Impact Assessment) – 3.5 Data breach e Severity Calculator – 3.6 La famiglia degli Standard ISO/IEC 27000

3.1 Sicurezza dei dati e cibersicurezza

Viviamo indubbiamente in quella che può essere definita, con espressione ormai diffusa, la *golden age of surveillance*. A determinare questa fase storica è lo sviluppo delle tecnologie digitali, che rendono possibile la raccolta e la conservazione di quantità di dati personali in misura esponenzialmente superiore rispetto al passato. Anche l'Unione Europea partecipa attivamente a questa dinamica, che si alimenta da due fronti principali: da un lato, gli Stati membri che, per finalità di sicurezza nazionale e attività di polizia, ricorrono sempre più frequentemente all'accesso a comunicazioni private e all'acquisizione di dati personali; dall'altro, le imprese – in particolare quelle operanti nel settore delle tecnologie dell'informazione e della comunicazione – le quali, in qualità di fornitori di servizi o sviluppatori di strumenti di intercettazione, costruiscono su tali pratiche modelli economici basati sulla commercializzazione dei dati e sulla diffusione di tecnologie di sorveglianza[256]. Le economie fondate sui dati e le nuove opportunità derivanti dall'evoluzione tecnologica stanno influenzando

[256] A. BONFANTI, *La protezione dei dati personali nell'era digitale: considerazioni alla luce del quadro giuridico internazionale in materia di business e diritti umani*, in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 2017, 18(3), 477-497.

profondamente i rapporti giuridici ed anche le modalità con cui gli Stati intervengono per rispondere all'esigenza di regolamentare fenomeni inediti. In particolare, l'esigenza di un rinnovato intervento pubblico si innesta su un impianto normativo e su competenze tradizionali, alle quali si stanno progressivamente affiancando nuovi strumenti.

Un elemento certamente innovativo nella risposta statale a tali esigenze è rappresentato dalla crescente attenzione riservata ai profili legati alla cibersicurezza, la cui fragilità è emersa chiaramente con l'avanzare della digitalizzazione.

La cibersicurezza viene oggi richiamata quale strumento essenziale per garantire l'affidabilità e la protezione delle attività, sia pubbliche che private, di natura economica o sociale, svolte attraverso l'impiego di tecnologie digitali e, più in generale, all'interno dello "spazio cibernetico"[257].

È ben noto che la sicurezza informatica consiste nell'adozione di strategie, strumenti e misure volte a proteggere sistemi hardware, software e dati da accessi non autorizzati, siano essi accidentali o intenzionali. L'obiettivo principale è assicurare la riservatezza delle informazioni, prevenendo utilizzi illeciti, alterazioni, diffusione non consentita o distruzione dei dati[258]. La cybersecurity o sicurezza informatica è dunque quel ramo dell'informatica che si occupa di analizzare e prevenire le minacce informatiche, di valutare il rischio derivante dall'utilizzo di strumenti informatici, di trovare soluzioni al fine di proteggere i nostri dati da possibili attacchi che potrebbero provocare danni diretti o indiretti[259]. Secondo lo standard UNI/EN ISO 10459/2015 la sicurezza può essere definita come lo

[257] A. SOLA, *Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale*, in *Media Laws*, 2022, 3, 386-404.
[258] A. IASELLI, M. IASELLI, *Nuove tecnologie, sicurezza e protezione dei dati*, Milano, Giuffrè Francis Lefebvre, 2024.
[259] G. CASCAVILLA, M. CONTI, *Cybersecurity: Uno stato dell'arte*, in *Formazione esperienziale: Proposte per la sicurezza digitale*, a cura di A. SURIAN, D. FRISON, Pensa MultiMedia, 2019, 13-18.

"*studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa, che possono danneggiare le risorse materiali, immateriali ed umane di cui l'azienda dispone e necessita per garantirsi un'adeguata capacità concorrenziale nel breve, medio e lungo periodo*."

Le questioni legate al trattamento dei dati, dalla raccolta alla gestione e circolazione, richiedono un approccio sistemico, capace di tutelare il delicato equilibrio tra sicurezza, trasparenza e rispetto dei principi democratici, tanto nelle modalità quanto nelle finalità del trattamento. In tale prospettiva, risulta sempre meno rilevante operare una rigida distinzione tra le diverse categorie di dati; ciò che assume centralità è, piuttosto, l'uso concreto che di quei dati viene fatto. Infatti, la classificazione tra dati personali, non personali, dati aperti o dati suscettibili di essere trattati come beni economici, specie laddove l'assenso al trattamento diviene condizione necessaria, spesso implicita, per l'accesso a servizi pubblici o privati (si pensi, ad esempio, alla profilazione), sembra oggi perdere peso sul piano strettamente giuridico, rendendo meno nette le distinzioni normative tra le varie tipologie. Dall'analisi integrata delle normative attualmente in vigore, emerge una tendenza verso un approccio unitario, orientato a valorizzare appieno il potenziale economico e sociale derivante dall'impiego e dal riutilizzo dei dati, inclusi quelli personali; questo avvicinamento tra categorie differenti di dati segna un'evoluzione significativa nella logica regolatoria. Di conseguenza, il parametro giuridico centrale si sposta verso il concetto di sicurezza digitale, inteso come fondamento essenziale per garantire sia la legittimità del trattamento dei dati, con la connessa tutela dei diritti fondamentali delle persone, sia per soddisfare le istanze di sicurezza pubblica, secondo una prospettiva coerente con l'assetto ordinamentale[260].

[260] R. D'AGOSTINO, *La gestione dei dati nell'era digitale: un difficile bilanciamento fra esigenze di sicurezza, trasparenza e solidarietà*, in *P.A. Persona e Amministrazione*, 2024, 14(1), 555–578.

Ogni giorno viene generata e raccolta una quantità straordinaria di dati da parte di soggetti pubblici e privati che, una volta analizzati, condivisi e riutilizzati, acquisiscono un valore sempre maggiore, ma allo stesso tempo diventano obiettivi particolarmente vulnerabili per attacchi informatici e violazioni della sicurezza digitale. Come evidenziato anche nel Rapporto Clusit 2024[261], il numero di attacchi cibernetici è in forte aumento: rispetto al 2019, nel 2023 si è registrato un incremento del 60% degli attacchi rilevati da fonti pubbliche, passando da 1.667 a 2.779. Anche a livello globale si è osservata una crescita dell'11%, mentre in Italia l'aumento è stato del 65%.

Questo scenario evidenzia una significativa espansione della superficie d'attacco, con conseguenze che incidono profondamente non solo su sistemi politici ed economici, ma anche su dimensioni essenziali della vita sociale. L'utilizzo improprio o doloso dei dati – soprattutto di quelli personali – contribuisce infatti ad alimentare forme di disuguaglianza digitale, dove i diritti fondamentali degli individui rischiano di essere compromessi o subordinati al potere delle tecnologie e delle piattaforme digitali. Nel contesto dell'evoluzione tecnologica continua, la rete e i servizi digitali offerti al suo interno si configurano sempre più frequentemente come obiettivi privilegiati di attacchi informatici (*cyber attacks*). Tali episodi non si limitano a compromettere il funzionamento o la disponibilità dei servizi, ma possono anche determinare gravi violazioni della riservatezza, integrità e disponibilità dei dati personali, dando luogo a fenomeni di *data breach* potenzialmente rilevanti.

In questa prospettiva, si delinea un nesso sempre più stretto tra la protezione delle infrastrutture digitali e la tutela delle informazioni personali. Tale interrelazione richiama con forza l'applicazione del quadro normativo in materia di protezione dei dati personali, trovando il suo fulcro, a livello europeo, nel Regolamento (UE) 2016/679 (GDPR), che disciplina, tra l'altro,

[261] A tal proposito si veda il Rapporto Clusit 2024.

le misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio[262]. Il considerando n. 83 rivela infatti la natura centrale del *principio di sicurezza*, come *rectius* alla tutela della persona: "*Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.*"

Il principio di sicurezza si trova cristallizzato all'interno dell'art. 32 del GDPR, secondo cui titolare e responsabile del trattamento devono adottare misure tecniche e organizzative adeguate al rischio, tenendo conto di: stato dell'arte tecnologica; costi di attuazione; natura, oggetto, contesto e finalità del trattamento; livello di rischio per i diritti e le libertà delle persone. Le misure di sicurezza possono includere:

- Pseudonimizzazione e cifratura dei dati personali.
- Capacità di garantire riservatezza, integrità, disponibilità e resilienza.
- Capacità di ripristino dei dati in caso di incidenti.
- Test e verifiche periodiche sull'efficacia delle misure adottate.

[262] F. CAMISA, A. SIMONCINI, *Il fattore umano e la regolazione della cybersecurity*, in *Mondo Digitale*, 2024, 1.

Nel valutare i rischi specifici è necessario individuare distruzione, perdita o modifica dei dati così come divulgazione o accesso non autorizzati, anche accidentali o illeciti. Nel contesto descritto titolare e responsabile devono poter garantire che chiunque tratti dati sotto la loro autorità sia istruito e agisca solo su loro indicazione, salvo obblighi di legge. L'adesione a codici di condotta o certificazioni può essere un elemento per dimostrare tala conformità[263].

Dal punto di vista normativo, l'Italia ha sviluppato nel tempo un quadro articolato per affrontare le sfide della sicurezza cibernetica. A partire dal DPCM del 24 gennaio 2013 (cosiddetto Decreto Monti), si è delineata una prima architettura nazionale per la protezione informatica. Tale assetto è stato progressivamente aggiornato, in particolare con il DPCM del 2017 (Decreto Gentiloni[264]). Tramite il cosiddetto Decreto Gentiloni, anche l'Italia ha proceduto nel compiere un importante passo avanti nel rafforzamento della sicurezza informatica. Il provvedimento ha infatti introdotto un programma nazionale volto allo sviluppo della cybersecurity, articolato in più fasi, in modo da permettere il potenziamento della resilienza digitale del Paese. Tra i principali effetti della riforma indicata, vi è il consolidamento del ruolo del Comitato Interministeriale per la Sicurezza della Repubblica (CISR), il quale è incaricato di emanare direttive strategiche finalizzate a innalzare il livello di protezione cibernetica a livello nazionale. In tale contesto, è stato istituito il Nucleo per la Sicurezza Cibernetica (NSC), organismo responsabile di assicurare una risposta coordinata e tempestiva agli incidenti informatici che possano compromettere la sicurezza nazionale, operando in stretta collaborazione con le strutture competenti dei vari ministeri[265].

---

[263] E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, Giuffrè, 2023.

[265] G. CASCAVILLA, M. CONTI, *Cybersecurity: Uno stato dell'arte*, in *Formazione esperienziale: Proposte per la sicurezza digitale*, a cura di A. SURIAN, D. FRISON, Pensa MultiMedia, 2019, 13–18.

Il d.lgs. 65/2018 (attuativo della Direttiva NIS[266] poi sostituita dalla direttiva NIS2 a partire da fine 2024), ha istituito il Perimetro di sicurezza nazionale cibernetica. Ulteriori rafforzamenti sono arrivati con il d.l. 105/2019, volto a garantire un elevato livello di protezione per le infrastrutture digitali critiche, pubbliche e private. Sebbene spesso trascurata o oggetto di interpretazioni errate, la connessione tra protezione dei dati personali e cibersicurezza si rivela in realtà profonda e strutturata. Tale rapporto sinergico ha oggi un riconoscimento normativo esplicito nel decreto-legge 14 giugno 2021, n. 82, che ha istituito l'Agenzia per la cybersicurezza nazionale.

In particolare, il decreto prevede forme specifiche di cooperazione tra l'Agenzia e il Garante per la protezione dei dati personali, anche attraverso la stipula di protocolli d'intesa e con la previsione di meccanismi di consultazione. Un esempio significativo di tale collaborazione è rappresentato dal protocollo siglato nel febbraio 2022, che disciplina – tra gli altri aspetti – le modalità di gestione e comunicazione delle violazioni dei dati personali (data breach)[267].

Con il decreto-legge 14 giugno 2021, n. 82, il legislatore ha voluto potenziare le misure di difesa cibernetica istituendo non solo l'Agenzia per la Cybersicurezza Nazionale (ACN), ma anche il Comitato interministeriale per la Cybersicurezza (CIC) e il Nucleo per la Cybersicurezza. Tali organismi rivestono un ruolo strategico nella protezione dello spazio digitale nazionale.

---

[266] Finalità principale di tale provvedimento normativo è garantire che tutti gli Stati membri dell'Unione, attraverso l'elaborazione e l'attuazione di strategie nazionali specifiche, siano in grado di affrontare e gestire – anche tramite il ripristino dei servizi – eventuali attacchi cibernetici di natura distruttiva. In quest'ottica, vengono identificati alcuni settori strategici di riferimento, tra cui figurano quello energetico, dei trasporti, della sanità, e altri. G. BORRIELLO, G. FRISTACHI, *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in *Rivista di Digital Politics*, 2022, 2(1-2), 157-178.

[267] F. RESTA, *Cybersicurezza e protezione dati: un rapporto ambivalente*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 67-70.

In particolare, l'ACN è investita della responsabilità di garantire la sicurezza informatica del Paese, sia in termini di prevenzione sia in termini di risposta agli incidenti, coordinando le Autorità competenti e curando la redazione della Strategia nazionale di cybersicurezza. Al CIC è demandato il compito di vigilare sull'attuazione di tale Strategia e di fornire supporto alla Presidenza del Consiglio nelle politiche relative al Perimetro di sicurezza nazionale cibernetica. Il Nucleo per la Cybersicurezza, infine, opera in stretta collaborazione con il Presidente del Consiglio, supportandolo nella gestione di eventuali situazioni di crisi derivanti da attacchi informatici.

Un ulteriore passo in questa direzione è stato compiuto con la legge 29 dicembre 2022, n. 197 (legge di bilancio 2023), che nei commi da 899 a 902 ha previsto l'attuazione operativa della Strategia nazionale di cybersicurezza, adottata formalmente con DPCM del 17 maggio 2022. A tale scopo, sono stati istituiti appositi fondi nel bilancio del Ministero dell'Economia e delle Finanze, destinati a sostenere l'intero piano di implementazione, segnalando una chiara volontà politica di consolidare l'infrastruttura normativa e operativa del Paese in ambito digitale[268].

Si precisa, sempre per quanto concerne aspetti relativi alla sicurezza, che la Direttiva 95/46/CE adottava un'impostazione statica nella regolamentazione della tutela e del trasferimento dei dati personali, basata principalmente su una concezione proprietaria del dato. In netta discontinuità, il legislatore europeo, con l'adozione del Regolamento (UE) 2016/679 (GDPR), ha optato per un approccio più dinamico e flessibile, introducendo due criteri fondamentali per determinare l'ambito di applicazione territoriale della normativa: il criterio dello stabilimento e il criterio del targeting.

Con il criterio dello stabilimento, non è più rilevante il luogo fisico in cui si svolge il trattamento dei dati, bensì la presenza di un'organizzazione

[268] SORRENTINO, A. F. SPAGNUOLO, *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 685-701.

stabilita nell'Unione Europea. Il criterio del targeting, invece, amplia ulteriormente il raggio di azione del GDPR, richiedendo l'applicazione della normativa anche ai soggetti extra-UE che, pur non essendo fisicamente presenti nell'Unione, offrono beni o servizi o monitorano il comportamento di persone che si trovano nel territorio dell'Unione stessa.

Di conseguenza, la disciplina europea si estende anche ai titolari e ai responsabili del trattamento che operano al di fuori dei confini comunitari, ma che rivolgono la loro attività a interessati situati nell'UE. In tal senso, il GDPR ha profondamente trasformato il ruolo dei soggetti che, a vario titolo, trattano dati personali, promuovendo una rilettura delle loro funzioni secondo un approccio sostanziale (*substance over form*), piuttosto che meramente formale.

Il quadro giuridico delineato si discosta così dalle tradizionali categorie civilistiche fondate sulla dicotomia tra diritto reale e obbligazione, sviluppando una struttura normativa a forte connotazione pubblicistica, il cui vertice è rappresentato dall'Autorità garante per la protezione dei dati personali. Considerando che l'obiettivo prioritario del GDPR è la salvaguardia dei diritti e delle libertà fondamentali delle persone fisiche cui i dati si riferiscono, emerge chiaramente la centralità della figura del titolare del trattamento, quale perno attorno al quale ruota l'intero sistema di responsabilità e garanzie previste dalla normativa[269].

Come autorevolmente evidenziato in dottrina[270], il confronto tra il Regolamento generale sulla protezione dei dati (GDPR) e alcune tra le più rilevanti normative in materia di cibersicurezza – quali la direttiva NIS (e la sua evoluzione NIS2), la direttiva PSD2 in ambito di servizi di pagamento

[269] F. LORÈ, *Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva?*, in *Amministrativ@mente - Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2024, 65-90.
[270] A. MANTELERO, G. VACIAGO*, Reconciling data protection and cybersecurity: An operational approach for business sector*, in, *Privacy and data protection in software services*, a cura di R. SENIGAGLIA, C. IRTI, A. BERNES, Springer, 2022, 97-110.

elettronico, e la direttiva eIDAS sull'identità digitale e i servizi fiduciari – mette in luce significative convergenze nei rispettivi modelli regolatori.

Un primo elemento comune è rappresentato dal ricorso all'analisi del rischio come criterio guida per la definizione e l'adeguamento delle misure di sicurezza da adottare. Tale approccio, fondato sulla proporzionalità e sulla prevenzione, costituisce un asse portante tanto del GDPR quanto della direttiva NIS2 e della normativa PSD2.

Un ulteriore punto di contatto è dato dall'applicazione del principio di "protezione dei dati fin dalla progettazione e per impostazione predefinita" (privacy by design e by default), che non trova applicazione esclusivamente nel contesto del GDPR, ma risulta recepito anche nei quadri normativi della PSD2 e della revisione della direttiva eIDAS.

Rilevante è poi la presenza generalizzata dell'obbligo di notificare le violazioni dei dati personali (data breach), istituto che si ritrova in tutte le discipline sopra richiamate. Analogo discorso vale per l'esigenza, trasversalmente riconosciuta, di predisporre adeguate procedure di continuità operativa e ripristino (*business continuity* e *disaster recovery*).

In definitiva, tali affinità evidenziano come vi sia un substrato procedurale e operativo condiviso che consente di superare una lettura settoriale e frammentaria dei diversi interventi normativi. Al contrario, esse suggeriscono la possibilità di una visione sistemica, improntata alla coerenza e all'integrazione tra normative apparentemente autonome ma in realtà profondamente interconnesse[271]. Ne deriva un'impostazione marcatamente preventiva in entrambi gli ambiti normativi, caratterizzata da obblighi di gestione del rischio che, con l'introduzione della direttiva NIS2, si estendono ora all'intera filiera della supply chain. In tale prospettiva, è emersa una responsabilizzazione progressiva degli operatori, chiamati a considerare la

[271] B. PONTI, *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 57-66.

protezione dei dati e la sicurezza dei sistemi non solo come adempimenti normativi, ma anche come elementi qualificanti della propria accountability e fattori strategici di competitività sul mercato. Un ulteriore elemento di convergenza tra i due plessi normativi è rappresentato dal ricorso alle certificazioni, che si inseriscono nell'architettura preventiva come strumenti di garanzia e trasparenza, rafforzando la fiducia degli utenti e delle autorità[272].

In linea con l'evoluzione della società verso la cosiddetta *Risiko-Gesellschaft*, teorizzata da U. Beck, la valutazione e la gestione dei rischi cibernetici occupano oggi una posizione centrale nelle agende tecnologiche e regolatorie della maggior parte degli Stati contemporanei.

Dal punto di vista normativo, ciò ha determinato il rafforzamento di un approccio *risk-based*, il quale ha trovato nell'ordinamento dell'Unione Europea un terreno particolarmente favorevole alla sua affermazione. Questo approccio ha assunto una portata via via più estesa, fino a divenire pervasivo, influenzando non soltanto la disciplina in materia di protezione dei dati personali, ma anche il crescente corpo normativo dedicato all'intelligenza artificiale.

In definitiva, la cibersicurezza manifesta oggi una marcata tendenza all'"esorbitanza": essa supera ampiamente la sua originaria configurazione, storicamente legata agli ambiti della cyber-guerra e del cyber-terrorismo, per estendersi a una pluralità di settori interconnessi con il più ampio e strategico concetto di sicurezza nazionale[273]. Gli attacchi cibernetici stanno diventando sempre più pericolosi: in una società digitalizzata e iperconnessa, fortemente dipendente dalla tecnologia, le conseguenze di un attacco informatico possono essere devastanti. Se la privacy è riconosciuta come un diritto fondamentale nell'Unione Europea, lo stesso deve valere per la

[272] F. RESTA, *Cybersicurezza e protezione dati: un rapporto ambivalente*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 67-70.
[273] A. ODDENINO, *Pervasività, centralità geopolitica e molteplicità delle istanze di tutela della cybersicurezza: elementi introduttivi*, in *Teoria e Critica della Regolazione Sociale/Theory and Criticism of Social Regulation*, 2024, 2(29), 15-24.

cibersicurezza: la protezione dei dati, delle reti e delle informazioni rappresenta infatti la condizione essenziale per poter esercitare altri diritti. Come affermava S. Rodotà a proposito della privacy in senso lato, essa è strettamente legata alla possibilità di godere del diritto di associazione, di espressione, di opinione, di movimento e così via. Se non siamo in grado di tutelare i dati che ci identificano come cittadini, elettori, lavoratori o semplicemente come membri di una comunità, rischiamo di esporci a forme di potere incontrollato, come la sorveglianza di massa, la manipolazione politica e la persuasione commerciale. Per questo motivo, privacy e cibersicurezza devono essere considerate presupposti indispensabili per l'effettivo esercizio della libertà di opinione, di associazione, di circolazione e di altri diritti fondamentali[274].

Alcuni settori particolarmente sensibili evidenziano questioni rilevanti in materia di tutela della privacy e sicurezza dei dati personali. Tra questi, il lavoro, dove la normativa protegge la libertà del lavoratore dalle ingerenze datoriali, fungendo da strumento di riequilibrio sociale; la pubblica amministrazione, che richiede il bilanciamento tra riservatezza individuale e trasparenza, come evidenziato dalla pronuncia Zanon n. 20/2019 della Consulta; il marketing e il telemarketing, nei quali emerge la necessità di contemperare libertà d'iniziativa economica e tutela della dignità e libertà individuale; infine, la sanità, settore in cui la pandemia ha reso particolarmente evidente la sfida di conciliare esigenze di salute pubblica e protezione dei dati personali sensibili, la cui divulgazione indebita può comportare discriminazioni e stigmatizzazioni[275]. Visti gli ampi settori soggetti a rischi in materia di violazione dei dati personali, è importante indicare come Il GDPR abbia inaugurato un nuovo paradigma nel modello

[274] A. DI CORINTO, *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in *Rivista italiana di informatica e diritto*, 2022, 4(1), 31-37.
[275] P. STANZIONE, *Cybersicurezza e protezione dei dati personali*, in *Iura & Legal Systems*, 2025, 7(2), 76-84.

sanzionatorio relativo alla protezione dei dati personali. Dalla sua entrata in vigore, le autorità di controllo europee hanno irrogato sanzioni che, con la normativa precedente, difficilmente sarebbero state comminate, o avrebbero avuto caratteristiche sostanzialmente diverse. La disciplina antecedente, infatti, non contemplava concetti ora centrali come accountability, privacy by design e by default, valutazioni d'impatto sulla protezione dei dati (DPIA), registro dei trattamenti o obblighi di notifica dei data breach[276].

Nell'attuale scenario segnato da una costante e crescente esposizione a minacce informatiche di natura tanto sofisticata quanto diffusa, la sicurezza dei sistemi digitali e la protezione dei dati personali non possono più essere considerate come ambiti separati o, peggio ancora, come concetti giuridici e tecnici astratti. Le violazioni dei dati, infatti, non costituiscono ipotesi teoriche, ma fenomeni concreti, tangibili e con ricadute dirette sulla vita di milioni di individui, incidendo in modo significativo sui loro diritti fondamentali e sulla fiducia che essi ripongono nei confronti delle istituzioni e degli operatori economici.

In tale prospettiva, risulta evidente che la sicurezza non possa dirsi effettivamente realizzata se non incorpora al proprio interno, in maniera organica e strutturale, misure idonee a garantire la protezione dei dati personali; allo stesso modo, la protezione dei dati, per essere sostanziale e non meramente formale, non può prescindere da un robusto e costante presidio di sicurezza informatica. Si tratta, dunque, di due dimensioni che si alimentano reciprocamente e che, pur mantenendo una propria autonomia concettuale, si configurano al contempo come presupposti indispensabili l'una per l'altra.

Sicurezza e protezione dei dati si rivelano, pertanto, non soltanto come valori essenziali a livello individuale – in quanto strettamente legati alla tutela

[276] B. BORRILLO, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *Dirittifondamentali.it*, 2020, 2, 326-356.

della sfera privata e alla garanzia di libertà fondamentali – ma anche come beni collettivi, senza i quali le società contemporanee rischiano di vedere compromessa la loro stessa capacità di funzionare, di innovare e di prosperare.

Ne deriva che non appare più sufficiente, né concettualmente né pragmaticamente, affrontare il rapporto tra sicurezza e protezione dei dati nei termini di un semplice bilanciamento tra interessi potenzialmente confliggenti; occorre piuttosto avviare una riflessione orientata a coglierne la progressiva e necessaria convergenza, nella consapevolezza che essi costituiscono le due facce di una stessa medaglia e che solo nella loro integrazione può dirsi compiuta una strategia efficace di governo del rischio digitale[277]. Il legislatore europeo ha progressivamente instaurato una significativa simmetria tra protezione dei dati e sicurezza cibernetica (come si afferma in questo paragrafo). Ciò è particolarmente evidente in alcuni istituti comuni al GDPR e alla normativa in materia di sicurezza delle reti e dei sistemi informativi, quali la direttiva NIS 1, la successiva NIS 2 e, più recentemente, il Cybersecurity Act (Regolamento 2019/881). In tale contesto, l'obbligo imposto agli Stati membri di garantire che gli operatori di servizi essenziali e i fornitori di servizi digitali adottino (sotto pena di rilevanti sanzioni) misure di sicurezza adeguate ai rischi specifici del settore trova origine già nella disciplina sulla protezione dei dati, sin dalla direttiva 95/46/CE, ed è stato ulteriormente rafforzato con l'entrata in vigore del GDPR, secondo un approccio basato sul rischio, cui corrisponde l'adozione di misure proporzionate ed efficaci. Tale affinità normativa si ritrova anche nel *Cyber Resilience Act*, approvato definitivamente il 12 marzo 2024, consolidando il principio secondo cui sicurezza cibernetica e protezione dei

[277] A. BOURKA, P. DROGKARIS, *Security meets data protection: From risk management to systems engineering*, in *15 years of ENISA: A success story*, Publications Office of the European Union, 2019, 7-25.

dati costituiscono due facce complementari di un medesimo paradigma di governance digitale europea[278].

3.2 Data Governance, definizione e funzioni

La questione della gestione dei dati sta assumendo un'importanza sempre più rilevante nella società contemporanea a causa dello sviluppo digitale che ha notevolmente ampliato la capacità di raccolta, organizzazione e circolazione dei dati stessi, sia da parte della pubblica amministrazione sia da parte di soggetti privati. In un contesto sempre più dematerializzato e deterritorializzato, espressione di una società fluida e liquida, i dati (inseriti in rete, generati e diffusi dagli individui, spesso in modo inconsapevole) rappresentano un elemento chiave di questa trasformazione, al punto da essere spesso definiti "il nuovo petrolio" della società odierna; una società sempre più orientata verso lo sviluppo della cosiddetta data economy, un modello economico nel quale istituzioni e imprese sono chiamate non solo a interpretare correttamente i dati per migliorare sensibilmente le proprie performance, ma anche per innovare e potenziare l'azione pubblica. Affinché ciò si realizzi, è fondamentale che i dati vengano scambiati all'interno di uno spazio digitale sicuro e che vengano correttamente compresi e valorizzati. In primo luogo, quindi, è necessario che i soggetti preposti alla gestione dei dati, siano essi pubblici o privati, si impegnino a raccoglierli, elaborarli (computarli) e a comunicare i risultati in conformità alla normativa vigente: si tratta delle cosiddette "3C" – *capture, compute, communicate* – su cui si fonda l'architettura della data economy. Tutto questo è reso possibile dall'utilizzo di internet, dei sistemi informatici, dalla diffusione globale del

[278] F. RESTA, *Cybersicurezza e protezione dati: un rapporto ambivalente*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 67-70.

Cloud Computing e dalla sua progressiva integrazione con le reti in un'ottica di *Cloud Integrated Network*[279].

I modelli sviluppati e applicati di governance dei dati sono diversi. In linea generale, la letteratura identifica tre modelli principali: il modello *laissez-faire*, sostenuto dall'idea di uno stato minimo, della primarietà e naturalità del mercato e dalla globalizzazione[280]; il modello dei *data commons*, che promuove la gestione collettiva e condivisa dei dati come bene comune[281]; e il modello dei *data trusts*, che rappresentano strumenti consolidati e affidabili, progettati per garantire che la condivisione dei dati avvenga in modo sicuro e nel reciproco interesse delle parti coinvolte[282].

ll Data Governance Act non fornisce una definizione di governance dei dati. Tuttavia, con questa formula, è possibile considerare tutto l'insieme di regole e mezzi che disciplinano l'uso dei dati, mediante procedimenti di condivisione, accordi e standard tecnici, fino all'istituzione di strutture e processi per la condivisione dei dati in modo sicuro, anche attraverso soggetti terzi[283]. Come puntualmente descritto, il governo della digital society passa necessariamente dalla data governance, da intendersi proprio come tutela delle libertà e dei diritti nelle diverse fasi di gestione e nelle differenti configurazioni dei dati[284].

Nell'ambito della teoria organizzativa e del management, siamo ormai ampiamente familiari con i concetti di governance dell'Information

---

[279] R. DAGOSTINO, *La gestione dei dati nell'era digitale: un difficile bilanciamento fra esigenze di sicurezza, trasparenza e solidarietà*, in *P.A. Persona e Amministrazione*, 2024, 14(1), 555-578.
[280] A. VOLPI, *Il Disastro come Mezzo*, in *Power and Democracy*, 2021, 2(2), 45-56.
[281] J.J. ZYGMUNTOWSKI, L. ZOBOLI, P.F. NEMITZ, *Embedding European values in data governance: a case for public data commons*, in *Internet Policy Review*, 2021, 10(3).
[282] R. K. LOMOTEY, S. KUMI, R. DETERS, *Data Trusts as a Service: Providing a platform for multi-party data sharing*, in *International Journal of Information Management Data Insights*, 2022, 2(1).
[283] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi Parlamentari e di Politica Costituzionale*, 2021, (209), 31-52.
[284] F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Università di Bologna, 358.

Technology (IT governance) e di governance aziendale (corporate governance). Il termine "governance" in senso generale fa riferimento all'insieme di pratiche e meccanismi attraverso cui un'organizzazione definisce, monitora e realizza le proprie strategie. Con l'IT divenuto elemento strutturale e imprescindibile per il funzionamento delle organizzazioni contemporanee, la governance dell'IT si configura come parte integrante delle strategie di business, ricadendo a pieno titolo nel più ampio quadro della governance societaria. Tuttavia, non esiste una definizione ufficiale e universalmente riconosciuta di cosa si intenda per *data governance*. Per rispondere a questo interrogativo, il presente studio si propone di richiamare alcune definizioni formulate da importanti ricerche ed organizzazioni, al fine di offrire una visione comparata e articolata del concetto[285].

Grazie alle analisi di R. Abraham[286], è possibile offrire una definizione dei termini "data governance" e delineare i contorni di questa disciplina, considerando i cambiamenti significativi verificatisi nel contesto digitale negli ultimi anni. È interessante innanzitutto notare la distinzione tra *data governance* e *data management*. I due termini vengono spesso utilizzati in modo intercambiabile, ma rappresentano concetti distinti. Diversi autori, tra cui Abraham et al. (2019), hanno chiarito questa differenza. La *data governance* si concentra sulla gestione efficace e sull'uso dei dati in linea con la strategia generale dell'IT, specificando quali decisioni devono essere prese in ambito di gestione dei dati e chi è responsabile di prenderle. Il *data management*, invece, si occupa dell'attuazione pratica di queste decisioni, garantendo che esse vengano eseguite e che le azioni siano correttamente implementate.

---

[285] M. AL-RUITHE, E. BENKHELIFA, K. HAMEED, *A systematic literature review of data governance and cloud data governance*, in *Personal and Ubiquitous Computing*, 2019, 23(5), 839-859.

[286] R. ABRAHAM, J. SCHNEIDER, J. VOM BROCKE, *Data governance: A conceptual framework, structured review, and research agenda*, in *International Journal of Information Management*, 2019, 49, 424-438.

Per data governance si intende innanzitutto l'esercizio di autorità e controllo sulla gestione dei dati. Essa ha l'obiettivo di implementare un'agenda aziendale incentrata sui dati, andando a massimizzare il valore delle risorse di dati all'interno di un'organizzazione e gestendo i rischi che si legano agli stessi. Se in passato la data governance era considerata un elemento facoltativo nel sistema aziendale o organizzativo, oggi assume un'importanza sempre maggiore nelle imprese e nelle istituzioni governative. Il cambiamento di paradigma nella data governance è in gran parte dovuto all'aumento esponenziale dei volumi di dati generati a livello globale ogni anno, provenienti da una molteplicità di fonti (si pensi ai sistemi IoT come i wearable devices, le piattaforme di social media, le applicazioni aziendali e i differenti sistemi di transazione digitale che iniziano ad essere presenti in tutti i settori). Trent'anni fa, solo l'1% delle informazioni prodotte era digitale, mentre oggi oltre il 94% di queste informazioni è digitale e proviene da diverse fonti. Il 2002 è considerato l'"inizio dell'era digitale", un periodo in cui si è assistito a un'esplosione di dispositivi e informazioni prodotti digitalmente. Il numero e la quantità delle informazioni raccolte sono aumentati notevolmente grazie alla crescita dei dispositivi che raccolgono tali informazioni[287]. Questa molteplicità di dati introduce una complessità che richiede nuove strategie di gestione e controllo, poiché il rischio di incongruenze tra i dati o di lavorare con dati di scarsa qualità cresce con la varietà delle fonti e la rapidità dei flussi informativi. Per questo motivo le aziende stanno introducendo sempre più di frequente strumenti di reportistica e analisi interne, andando a confermare una emersa necessità di comprensione comune dei dati in seno a tutta l'organizzazione. L'impatto di alcune normative come il Regolamento Generale sulla Protezione dei Dati (GDPR) aumenta la pressione sulle aziende affinché abbiano un controllo preciso su

[287] B. BERISHA, E. MËZIU, *Big data analytics in cloud computing: an overview*, Seminar paper on the subject "Cloud Computing", University of Prishtina "Hasan Prishtina", 2021.

quali dati sono stati archiviati, dove si trovano e come vengono utilizzati e, per questa ragione, le organizzazioni sono costrette a trovare soluzioni per superare le sfide legate alle principali problematiche che colpiscono il sistema: dati inaccurati e incompleti, architetture aziendali frammentate e sistemi obsoleti, nonché problemi di conformità alle normative vigenti. In sintesi, ricostruendo la descrizione degli autori, è possibile indicare la seguente definizione standard: "*la data governance definisce un quadro interfunzionale per gestire i dati come una risorsa strategica aziendale. In questo contesto, stabilisce diritti decisionali e responsabilità per il processo decisionale di un'organizzazione riguardo ai propri dati. Inoltre, la data governance formalizza politiche, standard e procedure sui dati e ne monitora la conformità*".

Anche altri studi confermano la definizione di data governance riportata, in quanto quest'ultima può essere ampiamente definita come l'insieme di regole e meccanismi di applicazione che disciplinano la raccolta, l'accesso, l'archiviazione e l'elaborazione di dati di terze parti[288]. Nel contesto descritto in cui digitalizzazione e Big Data hanno un ruolo da protagonisti, questo è un tema di importanza intuitiva e di estrema complessità: la capacità di raccogliere, combinare o sfruttare insiemi di dati può determinare il successo di aziende o paesi, offrire enormi opportunità o generare rischi che saranno poi difficilmente gestibili senza gli strumenti adeguati.

Tuttavia, la data governance è raramente discussa e ciò è imputabile in parte alla sua definizione vaga: non esiste una singola regolamentazione che disciplini il tema in modo completo, sebbene molte normative ne regolino alcune sezioni specifiche. In parte, questo è dovuto alla sua componente fortemente politica: data la dominanza delle piattaforme digitali, la data governance si traduce, nella maggior parte dei casi, in governance delle

[288] O. BORGOGNO, M. SAVINI ZANGRANDI, *Data governance and the regulation of the platform economy*, in *Questioni di Economia e Finanza (Occasional Papers)*, Banca d'Italia, 2021.

piattaforme, un'attività che, nella corsa globale verso la supremazia digitale, sfocia rapidamente in tensioni (geo)politiche. Weill e Ross (2004)[289], in un momento precedente, definiscono la governance IT come "*la specificazione dei diritti decisionali e delle responsabilità per incoraggiare comportamenti desiderabili nell'uso dell'IT*". La loro definizione comprende l'istituzione di un insieme di processi e la delega di autorità per fornire input e prendere decisioni. In questa descrizione della governance IT non vi è nessun elemento che la renda meno appropriata per il settore pubblico rispetto a quello privato. Alcuni fattori trainanti possono certamente cambiare, ma la definizione fondamentale rimane valida in entrambi i settori.

Weill e Ross delineano tre domande che dovrebbero essere affrontate in qualsiasi approccio efficace alla governance IT:

- Quali decisioni devono essere prese per garantire una gestione e un uso efficaci dell'IT?
- Chi dovrebbe prendere queste decisioni?
- Come verranno prese e monitorate queste decisioni?[290].

Secondo Brous et al. (2016)[291], la governance dei dati non si limita alla sola definizione di un quadro di riferimento, ma può anche essere applicata nella pratica. Gli autori analizzano 35 fonti, tra articoli di riviste, atti di conferenze e libri, al fine di individuare i principi fondamentali della governance dei dati. Da questa analisi emergono quattro principi chiave: organizzazione, allineamento, conformità e comprensione condivisa. Gli autori suggeriscono che questi principi possano essere utilizzati dai ricercatori

[289] P. WEILL, J. W. ROSS, *IT Governance: How top performers manage IT decision rights for superior results*, Harvard Business School, Boston, 2004.
[290] L. P. DIAMOND, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results* (review), in *International Journal of Electronic Government Research*, 2005, 1(4), 63-67.
[291] P. BROUS, M. JANSSEN, R. VILMINKO-HEIKKINEN, *Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles*, in *5th International Conference on Electronic Government and the Information Systems Perspective (EGOV)*, Porto, Portugal, September 2016, 115-125.

per concentrarsi sulle questioni fondamentali legate alla governance dei dati e dai professionisti per sviluppare strategie efficaci in questo ambito[292].

La data governance comprende quindi l'insieme di processi, politiche e standard che garantiscono che i dati siano accurati, coerenti, accessibili e protetti. Una governance efficace non si limita a promuovere un utilizzo responsabile ed etico delle informazioni, ma assicura anche che siano protette da accessi non autorizzati, corruzione o perdita. Integrare misure di sicurezza già nella progettazione dei sistemi di gestione dei dati permette alle organizzazioni di proteggere le informazioni lungo tutto il loro ciclo di vita, dalla raccolta alla conservazione, dal trattamento alla condivisione.

I framework di governance combinano tipicamente politiche, strumenti e processi volti a far rispettare i protocolli di sicurezza dei dati. Tra le pratiche più diffuse vi sono la classificazione e l'etichettatura dei dati, le politiche di controllo degli accessi, la cifratura delle informazioni, l'adozione di meccanismi di auditing e il rispetto delle normative di settore, come il GDPR in Europa, l'HIPAA negli Stati Uniti o il CCPA in California. Questi strumenti, applicati in maniera integrata, contribuiscono a creare un ambiente in cui la protezione dei dati non è un elemento aggiuntivo, ma un aspetto intrinseco della gestione stessa delle informazioni[293].

Una governance dei dati davvero efficace si basa su una serie di pratiche strettamente integrate tra loro, pensate per garantire che le informazioni siano gestite in modo sicuro, responsabile e conforme alle normative vigenti. In primo luogo, è necessario capire che tipo di dati si possiedono e quale valore hanno: questo implica un'attenta classificazione e un inventario accurato delle informazioni, distinguendo quelle più sensibili

[292] O. BENFELDT NIELSEN, *A Comprehensive Review of Data Governance Literature*, in *IRIS: Selected Papers of the Information Systems Research Seminar in Scandinavia*, 2017, 8(3), 120-133.
[293] S. R. JULAKANTI, N. S. K. SATTIRAJU, R. JULAKANTI, *Security by Design: Integrating Governance into Data Systems*, in *International Journal of Communication Networks and Information Security (IJCNIS)*, 2022, 14(2), 393-399.

da quelle meno critiche. Senza questa fase preliminare, diventa impossibile applicare misure di protezione adeguate.

A partire da questa conoscenza, occorre stabilire chi può accedere ai dati e in quali condizioni, definendo regole chiare che limitino l'accesso solo a chi ne ha effettivamente bisogno per svolgere le proprie funzioni. La responsabilità sulla gestione dei dati, nota come *data stewardship*, deve essere assegnata a persone o gruppi specifici, incaricati di garantire la qualità dei dati, la loro sicurezza e l'uso etico delle informazioni.

La gestione dei dati comporta anche una costante analisi dei rischi, volta a individuare potenziali vulnerabilità, valutarne la gravità e adottare strategie per ridurre le possibilità di incidenti o violazioni. Parallelamente, le organizzazioni devono assicurare un monitoraggio continuo e il rispetto delle normative, come il GDPR o il CCPA, così da prevenire sanzioni e tutelare gli interessati.

Infine, non meno importante, è la preparazione a eventuali emergenze. Stabilire procedure di gestione degli incidenti significa essere pronti a rispondere rapidamente a qualsiasi problema di sicurezza, minimizzando i danni e ripristinando la normale operatività nel minor tempo possibile. Insieme, queste pratiche costituiscono un approccio olistico alla governance dei dati, capace di combinare organizzazione, controllo e responsabilità, proteggendo le informazioni e rafforzando la resilienza dell'organizzazione nel suo complesso[294].

Se viene preso in esame il ruolo della data governance nelle piccole e medie imprese (PMI), la gestione dei dati diventa fondamentale per garantire che le decisioni siano prese correttamente e che le azioni siano realizzate in modo efficace. L'obiettivo delle PMI è massimizzare il valore dei propri dati, e per fare ciò, le organizzazioni sono costantemente alla ricerca di metodi per

[294] S. R. JULAKANTI, N. S. K. SATTIRAJU, R. JULAKANTI, Data Protection through Governance Frameworks, in *Journal of Computational Analysis and Applications*, 2023, 31(1), 158-162.

generare valore dai dati. La data governance rappresenta uno strumento fondamentale per misurare e monitorare gli aspetti legati all'uso dei dati, ma, a causa delle differenze nelle strutture organizzative, esistono molteplici modalità di implementazione. Di conseguenza, la data governance assume diverse definizioni a causa della complessità organizzativa, configurandosi come un quadro strutturato per la gestione delle decisioni, dei diritti e delle responsabilità relative all'uso dei dati nell'impresa. In generale, i dati generano valore solo se vengono utilizzati e analizzati, e la qualità dei dati riguarda la loro "idoneità all'uso", l'obiettivo è quello di massimizzare tale qualità[295].

A livello pubblico, attraverso una necessaria semplificazione, si possono distinguere tre principali ambiti normativi che appaiono fondamentali per plasmare il framework della data governance di un paese: controllo dei dati, sicurezza nazionale e politiche della concorrenza. Si consideri il ruolo della pianificazione urbanistica, della rete dei trasporti e della distribuzione dei servizi essenziali, come scuole e ospedali: in un contesto decisionale basato su dati, è naturale che le istituzioni pubbliche facciano affidamento su strumenti capaci di elaborare grandi quantità di informazioni. Anzi, trascurare tale opportunità rappresenterebbe un errore metodologico. Tuttavia, è fondamentale interrogarsi sulla natura dei dati utilizzati e sulle tecniche impiegate per la loro analisi. È noto da quasi un secolo che le statistiche sono influenzate dalle scelte soggettive di chi le raccoglie ed elabora. Lo stesso vale per l'analisi dei dati, che può essere facilmente orientata per avvalorare determinate soluzioni[296].

---

[295] R. OKORO, *Proposed data governance framework for small and medium scale enterprises (SMEs)*, in *Cornerstone: A Collection of Scholarly and Creative Works for Minnesota State University*, Master's thesis, Minnesota State University, Mankato, 2021.
[296] V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2018, 2, 1-7.

A questi settori è possibile ricondurre le iniziative legislative in seno all'Unione che sono state discusse nel capitolo I. La regolamentazione del controllo dei dati definisce le regole per l'accesso, l'uso e il riutilizzo dei dati. Le normative sulla sicurezza nazionale determinano quali tipi di dati e utilizzi siano interdetti (con una portata sempre più ampia). La regolamentazione della concorrenza sanziona i comportamenti e le pratiche commerciali dei "creatori di mercato" digitali (spesso, le piattaforme stesse). Questi settori legislativi hanno un impatto profondo sull'economia digitale e si sovrappongono in modo sostanziale: intervenire su uno di essi spesso porta a effetti imprevisti nell'ambito degli altri. Rafforzare la gestione dei dati nel settore pubblico rappresenta un passaggio di interesse fondamentale per garantire la sicurezza delle informazioni sensibili, ottimizzare l'erogazione dei servizi e consolidare la fiducia dei cittadini nelle istituzioni. Le amministrazioni si trovano oggi ad affrontare sfide complesse, tra cui la protezione dalle minacce informatiche, la frammentazione dei dati tra diversi sistemi e la necessità di rispettare normative sempre più rigorose. Per far fronte a queste criticità, è fondamentale sviluppare framework di governance coerenti e standardizzati, modernizzare le infrastrutture tecnologiche e promuovere competenze digitali tra i dipendenti pubblici. Solo attraverso un approccio strutturato e integrato sarà possibile costruire un ecosistema di dati pubblico sicuro, efficiente e trasparente, capace di sostenere le politiche e i servizi nel lungo periodo[297].

Il Data Management, aspetto complementare alla data Governance, citato all'inizio di questo paragrafo, viene definito dall'Associazione per il Data Management (DAMA), ovvero la principale organizzazione

[297] P. K. PEMMASANI, M. A. ABD NASARUDDIN, *Strengthening Public Sector Data Governance: Risk Management Strategies for Government Organizations*, in *International Journal of Modern Computing*, 2022, 5(1), 108-118.

internazionale per i professionisti della gestione dei dati[298], come la disciplina che: "*favorisce la diffusione e la comprensione dell'importanza della gestione dei dati attraverso la definizione ed il supporto di un framework per la governance dei dati. I professionisti del Data Management, implementando i principi e le best practices del DAMA, garantiscono alla propria organizzazione tutti i benefici legati agli investimenti ed alla corretta governance dei propri dati, tra cui il controllo delle informazioni chiave, il governo dei processi, la modellazione dei dati, il monitoraggio costante della qualità dei dati e la gestione dei metadati trasformando il dato stesso in un vero asset chiave.*[299]"

I paragrafi successivi esploreranno le operazioni relative alla governance e al management dei dati, con particolare attenzione alla sicurezza delle informazioni, alla valutazione dei rischi, alla realizzazione delle Data Protection Impact Assessments (DPIA) e all'applicazione dei calcolatori di gravità per le violazioni dei dati (Data Breach Severity Calculator).

In assenza di adeguati framework di governance dei dati, le imprese rischiano di perdere il controllo sulle proprie informazioni, esponendosi a una maggiore vulnerabilità nei confronti di attacchi informatici, violazioni dei dati e sanzioni. Di conseguenza, l'adozione di pratiche solide di data governance non è importante solo per garantire la conformità normativa, ma rappresenta anche uno strumento essenziale per proteggere efficacemente i dati in ambienti digitali sempre più complessi e interconnessi. Sebbene la governance dei dati e la cybersecurity siano spesso trattate come discipline separate, in realtà sono profondamente interconnesse. La governance dei dati

[298] S. MANCINI, I. MUMENI URBANI, M. PELLEGRINO, E. TRINCA, *Governance dei dati e dell'AI: una sinergia strategica per la PA*, in *Agenda Digitale 360*, 2 gennaio 2024, disponibile su: https://www.agendadigitale.eu, consultato da ultimo il 24.10.2025.
[299] DAMA ITALY, *Sito ufficiale dell'associazione italiana per la Data Management Association International (DAMA)*, https://dama-italy.org/, consultato da ultimo il 24.10.2025.

fornisce la struttura e le politiche necessarie per garantire una gestione corretta delle informazioni, mentre la cybersecurity mette a disposizione strumenti e procedure per proteggerle da accessi non autorizzati, furti o alterazioni. Integrare le pratiche di governance dei dati con quelle di cybersecurity consente alle organizzazioni di adottare un approccio più completo alla gestione del rischio, affrontando contemporaneamente gli aspetti tecnici e organizzativi della protezione dei dati.

Un solido framework di data governance può rafforzare significativamente la resilienza informatica di un'organizzazione in diversi modi. In primo luogo, assicura che i dati siano classificati correttamente in base alla loro sensibilità e importanza, permettendo l'applicazione di controlli di sicurezza adeguati a ciascun tipo di informazione e garantendo che i dati più sensibili ricevano il massimo livello di protezione.

In secondo luogo, i framework di governance definiscono controlli di accesso chiari, limitando l'accesso ai dati sensibili esclusivamente al personale autorizzato. Ciò riduce il rischio di minacce interne, come l'uso improprio dei dati da parte di dipendenti o collaboratori per sottrarre o divulgare informazioni confidenziali. Inoltre, la governance dei dati prevede meccanismi di monitoraggio e auditing dell'utilizzo dei dati, consentendo alle organizzazioni di rilevare tempestivamente potenziali violazioni della sicurezza. Il monitoraggio continuo dei modelli di accesso e utilizzo permette di identificare attività sospette e reagire rapidamente per mitigare l'impatto di un attacco informatico.

Infine, un framework solido di data governance facilita il recupero in seguito a un attacco, garantendo la corretta gestione dei backup e l'esistenza di piani di *disaster recovery*. In caso di attacchi ransomware o violazioni dei dati, le organizzazioni che adottano buone pratiche di governance possono

ripristinare più rapidamente i sistemi e ridurre al minimo i tempi di inattività[300].

3.3 Valutazione del rischio

3.3.1 Valutazione del rischio privacy

Nel contesto giuridico, il concetto di "rischio" è da tempo utilizzato come strumento di governance, sebbene la sua applicazione sia differente nei diversi settori regolamentati e nelle diverse aree geografiche. Detto ciò, è evidente il ricorso sempre più frequente al "rischio" come criterio privilegiato per definire le priorità normative e di enforcement dell'Unione Europea, in particolare nell'ambito dell'economia dei dati e delle tecnologie emergenti.

Ad esempio, il concetto di "approccio basato sul rischio" (*risk-based approach*) era già presente nella precedente normativa europea in materia di protezione dei dati personali, la Direttiva 95/46/CE, in particolare:

- Nell'articolo 8 (trattamento di categorie particolari di dati).
- Nell'articolo 17 (misure di sicurezza).
- Nell'articolo 18 (procedura di notifica).
- E nell'articolo 20 (controlli preliminari delle autorità di protezione).

Il suo successore, il Regolamento Generale sulla Protezione dei Dati (GDPR), integra e arricchisce il concetto di rischio in maniera più ampia e strutturata[301].

Il Regolamento Europeo in materia di protezione dei dati personali ha segnato un cambiamento significativo di approccio e prospettiva nella tutela dei dati personali, introducendo un modello fondato sulla responsabilizzazione del titolare del trattamento, secondo il principio della

[300] V. K. S. ANIL, A. B. BABATOPE, *The Role of Data Governance in Enhancing Cybersecurity Resilience for Global Enterprises*, in *World Journal of Advanced Research and Reviews*, 2024, 24(1), 1420-1432.
[301] O. KOKOULINA, *Challenges in Digital Compliance: Risk Assessment and Fundamental Rights under the GDPR and the EU AI Act*, in *CEUR Workshop Proceedings*, 2024.

cosiddetta “accountability”. Il sistema delineato dal GDPR stabilisce che la protezione dei dati personali non sia più garantita attraverso la semplice osservanza di principi minimi fissati a livello nazionale, ma richiede una condotta attiva da parte del titolare del trattamento, il quale è chiamato a mettere in atto misure adeguate e coerenti con le finalità del trattamento e con il livello di rischio per i diritti e le libertà delle persone fisiche, secondo il cosiddetto *risk-based approach*. Con l’introduzione del GDPR, si è superato il semplice adempimento formale da parte del titolare del trattamento, passando ad un vero e proprio sistema che impone a chiunque gestisca dati personali l’adozione di misure tecniche e organizzative volte a garantirne la protezione. Tali misure devono dimostrare l’effettiva attuazione e l’efficacia di un modello di *compliance* integrata, fondato sull’analisi del rischio condotta dal soggetto obbligato, che può essere una persona fisica, giuridica, un ente o un’istituzione. Ciò significa che qualsiasi titolare coinvolto nel trattamento di dati personali, secondo i principi stabiliti dal Regolamento europeo del 2016, deve essere in grado, in ogni momento, di dimostrare di aver adottato misure conformi ai requisiti previsti dal GDPR, mettendo al centro i diritti e le libertà della persona fisica a cui i dati si riferiscono[302].

La valutazione e la gestione del rischio si sono affermate come campo scientifico diversi anni fa e sono stati sviluppati principi e metodi per concettualizzare, valutare e gestire il rischio. Tali principi e metodi rappresentano ancora oggi in larga misura le fondamenta di questo campo, ma sono stati fatti molti progressi, legati sia alla matrice teorica che ai modelli e alle procedure pratiche[303]. In breve, si può affermare che al rischio si possono attribuire due significati: uno vernacolare e uno più tecnico. Nell'accezione vernacolare, il rischio viene solitamente definito come un pericolo futuro e possibile, cioè come “un pericolo eventuale che può essere

[302] R. FLOREANI, S. PETRUSSI, *Il GDPR in ambito assicurativo*, vol. 2, Giuffrè, 2025.
[303] T. AVEN, *Risk assessment and risk management: Review of recent advances on their foundation*, in *European Journal of Operational Research*, 2016, 253(1), 1-13.

previsto solo in parte". In senso tecnico, tuttavia, il rischio può essere visto come una nozione duplice. È utilizzato per prendere decisioni basate sulla valutazione di eventi futuri. I suoi elementi costitutivi sono due operazioni distinte ma unite: la previsione di eventi futuri (sia negativi che positivi) e la presa di decisioni sulla base di essi. Si può quindi sostenere che "*qualsiasi decisione relativa al rischio comporta due elementi distinti e tuttavia inseparabili: i fatti oggettivi e un'opinione soggettiva sull'opportunità di ciò che si può guadagnare, o perdere, con la decisione*[304]". Nel contesto in esame, i rischi sono gli effetti negativi che si discostano dagli obiettivi attesi e che derivano dal verificarsi di eventi incerti. Il rischio, quindi, è un concetto composito, che raggruppa in sé tre aspetti diversi: possibilità, conseguenza e contesto. Tutti e tre contribuiscono ad ogni valutazione o quantificazione del rischio[305].

Secondo il WP29, "*un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità*[306]". Il fatto che si debba tenere conto sia della "probabilità" che della "gravità" è menzionato anche nei considerando 75 e 76 del GDPR. L'uso del termine "rischio", come già indicato, fa parte dell'approccio adottato dal legislatore europeo nel GDPR, verso una protezione dei dati più proattiva, scalabile ed efficace. Nonostante la sua importanza, si ricorda che il rischio non ha una definizione giuridica nell'ambito del quadro giuridico generale dell'UE sulla protezione dei dati personali (GDPR). Il legislatore ci fornisce esempi di

[304] R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, 34(2), 279-288.
[305] S. CANALE, C. FABIANO, S. LEONARDI, *Il concetto di rischio e gli ambiti applicativi dell'analisi del rischio*, *Istituto Strade Ferrovie Aeroporti*, Quaderno n. 100, 1998.
[306] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (WP 248 rev. 01)*, Commissione Europea, 13 ottobre 2017.

rischi (come appare nei considerando 75[307] e 91[308] del GDPR), ma non fornisce gli strumenti per valutare altre tipologie di rischi, la loro gravità e la loro probabilità, in modo oggettivo e coerente.

Il principio di responsabilizzazione (*accountability*) sancito all'articolo 5, paragrafo 2 del GDPR, recita: "*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilizzazione")*." In altri termini, il titolare deve garantire la conformità ai principi del trattamento dei dati personali e deve poter dimostrare concretamente tale conformità. Il *titolare del trattamento*[309], come

[307] Il considerando 75 del GDPR elenca situazioni che possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, ovvero: "*discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*."

[308] Il considerando 91 indica una situazione di 'rischio' con particolare riferimento ai: "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti.*"

[309] In linea di principio, non vi è alcuna limitazione rispetto al tipo di soggetto che può assumere il ruolo di titolare del trattamento, ma nella pratica si tratta solitamente dell'organizzazione nel suo complesso, e non di una singola persona al suo interno (come l'amministratore delegato, un dipendente o un membro del consiglio di amministrazione), ad agire come titolare. Il titolare è il soggetto che decide alcuni elementi chiave del trattamento. La titolarità può essere stabilita dalla legge oppure derivare da un'analisi degli elementi fattuali o delle circostanze del caso.
Il titolare determina le finalità e i mezzi del trattamento, ovvero il "perché" e il "come" del trattamento stesso. Deve decidere sia sulle finalità sia sui mezzi. Tuttavia, alcuni aspetti più pratici dell'attuazione (i cosiddetti "mezzi non essenziali") possono essere lasciati al responsabile del trattamento. Non è necessario che il titolare abbia effettivamente accesso ai

definito dal GDPR, è il soggetto che determina "le finalità e i mezzi del trattamento di dati personali" (art. 4, par. 7). Quest'ultimo è quindi il soggetto su cui ricade la responsabilità di assicurare che i trattamenti siano conformi ai principi stabiliti dal diritto dell'Unione in materia di protezione dei dati. Tale concetto è fondamentale perché **"***il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure*" (considerando 74 del GDPR). In sostanza, questo passaggio serve a chiarire l'attribuzione delle responsabilità. Sebbene il concetto di *accountability* non sia una novità nel contesto della protezione dei dati, il cambiamento introdotto dal GDPR riguarda il modo in cui il legislatore ha scelto di strutturare un sistema di conformità. Questo avviene, tra l'altro, attraverso la concretizzazione del principio di responsabilizzazione sia mediante un obbligo generale all'articolo 24, sia attraverso obblighi più specifici (ad esempio: la nomina del Responsabile della Protezione dei Dati, le Valutazioni d'Impatto sulla Protezione dei Dati – DPIA, e il principio della *privacy by design*). Tutti questi strumenti hanno una caratteristica comune: propongono misure e meccanismi concreti che promuovono un approccio proattivo, agevolano l'attuazione del principio di *accountability* e quindi rendono possibile sia il rispetto della normativa sia la dimostrazione della conformità stessa. Tali obblighi non introducono nuovi principi, ma rappresentano piuttosto strumenti per l'applicazione efficace dei principi già esistenti in materia di protezione dei dati[310]. Come noto, l'accountability si articola in due distinti obblighi cumulativi: il primo consiste nell'osservanza di una disposizione

dati trattati per essere qualificato come tale. European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Versione 2.1)*, 7 luglio 2021.

[310] K. DEMETZOU, *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, in *CEO Succession, Leadership, and (Dis)similarity*, in *IFIP Advances in Information and Communication Technology*, 2019, pp. 137-154

normativa, mentre il secondo riguarda la capacità del titolare del trattamento di fornire prova del proprio rispetto di tale disposizione. Di conseguenza, per aderire a questo principio, il titolare è generalmente tenuto a predisporre e conservare un'ingente quantità di documentazione, adottando quindi un atteggiamento proattivo.

Traslando il concetto di accountability nell'ambito della sicurezza informatica, il primo obbligo sarà rappresentato dalla definizione e attuazione di misure di sicurezza "appropriate", secondo quanto previsto dall'articolo 32 del GDPR, mentre il secondo riguarderà la capacità di attestare la conformità e l'adeguatezza di tali misure. Per quanto si possa ritenere che l'accountability, esplicitamente disciplinata dagli articoli 5(2) e 24 del GDPR, considerata un principio fondamentale della normativa in materia di protezione dei dati personali, non rappresenti di per sé una misura di sicurezza, essa costituisce comunque un presupposto essenziale attorno al quale dovrebbero essere strutturate tutte le misure di sicurezza, siano esse di tipo tecnico oppure organizzativo[311].

Il processo di risk management parte dalla tipologia di dati personali trattati e dalle attività di trattamento a cui sono sottoposti. Successivamente vengono individuate le minacce potenziali, e i rischi vengono stimati sulla base di diversi fattori che ne influenzano la probabilità e l'impatto.

In seguito, i rischi vengono valutati, prioritizzati, e si adottano varie contromisure, come:

- Privacy controls (misure tecniche e organizzative).
- PETs (Privacy-Enhancing Technologies).

Queste hanno la finalità di mitigare i rischi. Infine, i rischi vengono documentati e monitorati nel tempo[312].

---

[311] J. S. VANEGAS, *La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR*, in *Rivista Italiana di Informatica e Diritto*, 2020, 2(2), 5-14.
[312] Y. S. MARTÍN, A. KUNG, *Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering*, in *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2018, 108-111.

Il GDPR adotta un approccio coerente e basato sul rischio in numerose sue disposizioni (in particolare negli articoli 24, 25, 32 e 35) con l'obiettivo di individuare misure tecniche e organizzative adeguate a proteggere le persone fisiche e i loro dati personali, nonché per garantire la conformità ai requisiti del Regolamento. I soggetti da proteggere restano invariati (le persone fisiche, attraverso la tutela dei loro dati personali), così come i rischi (per i diritti degli interessati) e le condizioni da considerare (natura, ambito, contesto e finalità del trattamento). L'art. 32 del Regolamento è interessante in questo contesto poiché indica le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio che il titolare del trattamento e il responsabile del trattamento devono mettere in atto, le quali comprendono tra l'altro, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento[313]. Di fatto, il GDPR non indica un elenco chiuso e rigido, ma fa alcuni esempi di misure che possono essere adottate, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura dei dati trattati e della probabilità e gravità dei rischi per i diritti e le libertà degli interessati.

Nel valutare i rischi ai fini dell'applicazione dell'articolo 25 (Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita), il titolare del trattamento deve identificare i rischi per i diritti degli interessati derivanti da eventuali violazioni dei principi del trattamento, e valutarne la probabilità e la gravità, al fine di adottare misure efficaci per

[313] M. IASELLI, V. IASELLI, *Nuove tecnologie, sicurezza e protezione dei dati*, Milano, Giuffrè Francis Lefebvre, 2024.

mitigarli. Il rischio, infatti, non è un'entità astratta. Ha sempre un'origine precisa, che può trovarsi tanto all'interno delle strutture che gestiscono i dati quanto all'esterno, in contesti difficilmente controllabili. Non meno rilevante è la natura del rischio stesso, che come precedentemente evidenziato assume forme diverse: dalla perdita di informazioni sensibili fino all'uso distorto di dati apparentemente innocui. Ciò che conta, tuttavia, non è solo identificarlo, ma comprenderne la gravità, cioè l'ampiezza delle conseguenze che potrebbe produrre, e la probabilità che esso si verifichi concretamente. Una valutazione sistematica e approfondita del trattamento è essenziale durante l'analisi dei rischi. Ad esempio, il titolare può valutare i rischi specifici connessi all'assenza di un consenso liberamente prestato (che rappresenta una violazione del principio di liceità) nel trattamento dei dati personali dei minori, considerati un gruppo vulnerabile, in assenza di un'adeguata base giuridica. In tali casi, il titolare dovrà adottare misure appropriate per affrontare e mitigare efficacemente i rischi connessi a questo specifico gruppo di interessati[314]. Dunque, il principio di accountability attribuisce responsabilità ai titolari del trattamento, i quali dovranno adottare comportamenti proattivi e capaci di dimostrare l'effettiva adozione di misure finalizzate a garantire l'applicazione del regolamento. La disciplina ha inoltre previsto una serie di strumenti a disposizione dei titolari per dimostrare l'osservanza delle prescrizioni a loro carico e adempiere all'onere probatorio imposto dal principio di responsabilizzazione. Così, in base all'art. 24 del regolamento, l'adesione a codici di condotta o a meccanismi di certificazione può essere utilizzata come elemento utile a comprovare il rispetto degli obblighi del titolare del trattamento. Tale adesione può inoltre favorire la trasparenza del trattamento, con un conseguente aumento della fiducia da

[314] European Data Protection Board (EDPB), *Linee guida WP 250: "Protezione dei dati fin dalla progettazione e per impostazione predefinita" (Versione 2.0)*, 2021.

parte degli interessati, che, grazie alla certificazione, possono valutare con rapidità il livello di protezione dei propri dati[315].

3.3.2 Gli strumenti di valutazione del rischio

Gli strumenti di valutazione del rischio possono contribuire a prevedere una vasta gamma di esiti. Le istituzioni finanziarie, ad esempio, li utilizzano per stimare l'affidabilità creditizia dei clienti o addirittura per prevedere il rischio di insolvenza o fallimento. Anche il settore industriale (come i produttori) e i fornitori di infrastrutture critiche (come quelli della distribuzione energetica) impiegano strumenti di valutazione del rischio per identificare vulnerabilità dei sistemi e valutarne il potenziale impatto.

Esistono tuttavia molte altre applicazioni, come la valutazione del rischio sanitario, della sicurezza e così via. In modo analogo, anche i meccanismi di valutazione del rischio per la privacy sono fondamentali nei sistemi progettati per rafforzare la protezione dei dati personali e ridurre i rischi in questo ambito (in questo contesto si intendono i rischi per l'interessato e non per il titolare). Tali meccanismi di analisi del rischio privacy sono essenziali per prevenire o mitigare le violazioni dei dati[316]. Come sottolineato dall'ENISA[317] la gestione del rischio per la sicurezza delle informazioni è il processo di identificazione, quantificazione e gestione dei rischi legati alla sicurezza informatica a cui un'organizzazione è esposta. Al centro di questo processo vi è la valutazione del rischio per la sicurezza, seguita dal trattamento del rischio, dalla sua accettazione e comunicazione. Un rischio per la sicurezza delle informazioni è dato dalla combinazione tra la probabilità che una minaccia si concretizzi e l'impatto che tale minaccia

---

[315] B. BORRILLO, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *Dirittifondamentali.it*, 2020, 2, 326-356.
[316] P. SILVA et al., *Privacy risk assessment and privacy-preserving data monitoring*, in *Expert Systems with Applications*, 2022, 200.
[317] ENISA, *Online Platform for Security of Personal Data Processing: Reinforcing trust and security in the area of electronic communications and online services*, December 2019.

può avere sull'organizzazione. Vi sono standard riconosciuti, come ISO/IEC 27005:2018 e NIST 800-39, che hanno contribuito allo sviluppo di metodi, strumenti e applicazioni pratiche in questo ambito.

Un esempio significativo dell'approccio operativo promosso dall'ENISA è rappresentato dalla piattaforma online per la sicurezza del trattamento dei dati personali, sviluppata dall'agenzia come strumento pratico di valutazione dei rischi e di individuazione delle misure di sicurezza più adeguate. Sebbene tale servizio non sia più attualmente fornito dall'Agenzia, le caratteristiche e la metodologia che lo sorreggevano continuano a costituire un modello di riferimento, offrendo un quadro metodologico replicabile e coerente con i principi dell'art. 32 del GDPR. In questo senso, l'esperienza maturata con l'uso della piattaforma mantiene ancora oggi un valore paradigmatico, poiché ha contribuito a tradurre in procedure concrete il delicato passaggio dal piano astratto delle regole al livello operativo della gestione della sicurezza dei dati. La piattaforma online sviluppata dall'ENISA traduceva in pratica le diverse fasi dell'approccio basato sul rischio delineato dall'Agenzia, guidando i soggetti interessati (tipicamente titolari e responsabili del trattamento) in un percorso di valutazione del livello di rischio per la sicurezza e nella conseguente individuazione di misure tecniche e organizzative proporzionate. Lo strumento offriva, inoltre, la possibilità di condurre un *self-assessment* sulla sicurezza, consentendo all'organizzazione di verificare la coerenza tra le misure adottate e il livello di rischio percepito o individuato. La platea di riferimento era dunque molto ampia: non solo operatori economici e istituzionali, ma anche le stesse Autorità di protezione dei dati, che potevano avvalersi della piattaforma come supporto per monitorare e rafforzare la sicurezza del trattamento dei dati personali. Va precisato che la piattaforma online elaborata dall'ENISA era specificamente concepita come strumento di supporto per la sicurezza del trattamento dei dati personali e non poteva, dunque, essere confusa con una Data Protection Impact Assessment (DPIA). Quest'ultima, infatti, si caratterizza per una

portata ben più ampia, volta a valutare l'intero ciclo di vita di un trattamento e i relativi impatti sui diritti e le libertà fondamentali degli interessati, mentre l'iniziativa ENISA si concentrava unicamente sulla misurazione e gestione del rischio in termini di sicurezza informatica[318].

Il primo passo per effettuare una valutazione del rischio in materia di protezione dei dati personali secondo il modello dell'ENISA consiste nella precisa individuazione dell'operazione di trattamento e nel contestuale inquadramento del suo ambito applicativo. Tale attività si configura come momento imprescindibile, poiché consente al titolare o al responsabile del trattamento di delimitare i confini funzionali e organizzativi del sistema di trattamento oggetto di analisi. In tale prospettiva, risulta necessario prendere in considerazione le diverse fasi del ciclo di vita del dato (raccolta, conservazione, utilizzo, trasferimento, cancellazione), nonché gli elementi correlati, quali i destinatari, i mezzi e le infrastrutture impiegate. La finalità di questa prima fase (step 1) è, dunque, quella di garantire una comprensione sistematica e coerente del trattamento, così da porre solide basi per le successive fasi valutative.

Tabella 1 Individuazione dell'operazione di trattamento secondo il modello ENISA.

Quesito	**Finalità conoscitiva**
1. Qual è l'operazione di trattamento di dati personali?	Stabilire se sia necessario condurre processi di valutazione del rischio distinti in presenza di operazioni di trattamento eterogenee.
2. Quali sono le tipologie di dati personali oggetto di trattamento?	Individuare la natura dei dati trattati e desumere una prima indicazione circa i potenziali livelli di rischio.

[318] ENISA, *Handbook on Security of Personal Data Processing*, 2017.

3. Qual è la finalità perseguita dal trattamento?	Definire i limiti sostanziali e funzionali del trattamento in rapporto allo scopo dichiarato.
4. Quali mezzi vengono utilizzati per il trattamento dei dati personali?	Identificare le modalità operative e gli strumenti utilizzati (risorse interne, soluzioni esternalizzate, ecc.).
5. Dove viene effettuato il trattamento dei dati personali?	Determinare l'ubicazione del trattamento, al fine di valutarne le implicazioni in termini di rischio.
6. Quali sono le categorie di soggetti interessati coinvolti?	Definire le categorie di interessati (clienti, utenti, dipendenti, ecc.) ai quali i dati si riferiscono.
7. Chi sono i destinatari dei dati trattati?	Individuare i destinatari dei dati e le condizioni che legittimano i trasferimenti effettuati.

Nel rispondere a queste domande, un'organizzazione deve tenere in considerazione le diverse fasi del trattamento dei dati (raccolta, conservazione, utilizzo, trasferimento, eliminazione, ecc.) e i relativi parametri. Una volta delineata l'operazione di trattamento e il relativo contesto, il titolare o il responsabile del trattamento è chiamato a valutare l'impatto potenziale che un incidente di sicurezza potrebbe arrecare ai diritti e alle libertà degli interessati. Tale incidente può consistere in una violazione della riservatezza, dell'integrità o della disponibilità dei dati personali.

Considerata la natura eterogenea e spesso peculiare dei trattamenti, la metodologia adottata si fonda su un approccio qualitativo, basato sulla conoscenza approfondita del sistema di trattamento da parte dell'organizzazione. La valutazione prende in esame variabili rilevanti, quali tipologia e volume dei dati, criticità del trattamento, caratteristiche specifiche

del titolare o del responsabile, caratteristiche degli interessati e grado di identificabilità dei soggetti coinvolti.

L'analisi confluisce, infine, in una classificazione dell'impatto secondo quattro livelli predefiniti: basso, medio, alto e molto alto.

Tabella 2 Classificazione dell'impatto secondo il modello ENISA.

Livello di impatto	**Descrizione**
Basso	Gli interessati possono subire lievi disagi, facilmente superabili senza particolari conseguenze (es. tempo perso per reinserire informazioni, fastidi o irritazioni).
Medio	Gli interessati possono incontrare disagi significativi, superabili con qualche difficoltà (es. costi aggiuntivi, impossibilità temporanea di accedere a servizi, timori, stress, lievi disturbi fisici).
Alto	Gli interessati possono subire conseguenze rilevanti, superabili solo con notevoli difficoltà (es. appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni patrimoniali, perdita dell'impiego, citazioni in giudizio, peggioramento delle condizioni di salute).
Molto Alto	Gli interessati possono subire conseguenze gravi o addirittura irreversibili, non sempre superabili (es. impossibilità di lavorare, disturbi psicologici o fisici di lunga durata, morte).

La tabella che segue (step 2) può essere utilizzata per valutare separatamente l'impatto derivante dalla perdita di riservatezza, integrità e disponibilità.

Al termine di questa valutazione si otterranno tre diversi livelli di impatto (uno per ciascun aspetto: riservatezza, integrità e disponibilità). Il livello più alto tra questi viene considerato come il risultato finale della valutazione dell'impatto (ovvero il punto di riferimento per decidere le misure tecniche e organizzative necessarie a ridurre il rischio), in relazione all'intero trattamento dei dati personali. Questo perché basta un solo aspetto critico per mettere a rischio i diritti e le libertà delle persone interessate.

Tabella 3 Impatto derivante dalla perdita di riservatezza, integrità e disponibilità.

N°	**Domanda di valutazione**	**Aspetto considerato**	**Livelli di impatto possibili**
Impatto n°1	Si invita a riflettere sull'impatto che una divulgazione non autorizzata dei dati personali (perdita di riservatezza) – nel contesto dell'attività svolta – potrebbe avere sull'individuo ed esprimere una valutazione.	Riservatezza (confidentiality)	Basso / Medio / Alto / Molto alto
Impatto n°2	Si invita a riflettere sull'impatto che una modifica non autorizzata dei dati personali (perdita di	Integrità (integrity)	Basso / Medio / Alto / Molto alto

	integrità) – nel contesto dell'attività svolta – potrebbe avere sull'individuo ed esprimere una valutazione.		
Impatto n°3	Si invita a riflettere sull'impatto che una distruzione o perdita non autorizzata dei dati personali (perdita di disponibilità) – nel contesto dell'attività svolta – potrebbe avere sull'individuo ed esprimere una valutazione.	Disponibilità (availability)	Basso / Medio / Alto / Molto alto

Un passaggio ulteriore nella metodologia di analisi del rischio elaborata dall'ENISA (step 3) consiste nell'individuazione delle possibili minacce e nella valutazione della probabilità che si verifichino. Con "minaccia" si intende qualsiasi circostanza o evento in grado di compromettere la sicurezza dei dati personali, incidendo, come già menzionato, sulla loro riservatezza, integrità o disponibilità.

In questa fase, il titolare (o il responsabile del trattamento) è chiamato a comprendere i rischi derivanti tanto dall'ambiente esterno quanto da quello interno all'organizzazione, al fine di stimarne la probabilità di accadimento.

L'approccio proposto dall'ENISA prevede, come indicato nelle tabelle che precedono, più livelli di probabilità di occorrenza della minaccia: bassa (improbabile che si verifichi), media (possibile che si verifichi) e alta (probabile che si verifichi). Per facilitare l'applicazione pratica, in particolare

da parte delle piccole e medie imprese, vengono individuate quattro aree di osservazione prioritarie:

- Risorse di rete e infrastrutture tecniche (hardware e software);
- Processi e procedure connessi al trattamento;
- Soggetti e attori coinvolti nell'operazione di trattamento;
- Settore di attività e scala del trattamento.

Attraverso tali dimensioni di analisi, accompagnate da specifici quesiti guida (come indicato nella tabella che segue), l'organizzazione può condurre una valutazione più consapevole e strutturata delle minacce e della loro concreta probabilità di materializzazione.

Tabella 4 Valutazione delle minacce secondo il modello ENISA.

Area di valutazione	**Domanda guida**
A. Risorse di rete e tecniche (hardware e software)	1. Ci sono parti del trattamento di dati personali che vengono effettuate tramite internet? 2. È possibile accedere a un sistema interno di trattamento dei dati personali attraverso internet (es. per alcuni utenti o gruppi di utenti)? 3. Il sistema di trattamento dei dati personali è interconnesso con altri sistemi o servizi informatici esterni o interni all'organizzazione? 4. Persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati? 5. Il sistema di trattamento dei dati personali è stato progettato,

	implementato o mantenuto senza seguire le *best practices* rilevanti?
B. Processi/procedure legate al trattamento dei dati	6. I ruoli e le responsabilità in materia di trattamento dei dati personali sono vaghi o non chiaramente definiti? 7. L'uso accettabile della rete, dei sistemi e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito? 8. Ai dipendenti è consentito portare e utilizzare i propri dispositivi per collegarsi al sistema di trattamento dei dati personali? 9. Ai dipendenti è consentito trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione? 10. Le attività di trattamento dei dati personali possono essere svolte senza che vengano creati file di log?
C. Parti e persone coinvolte nell'operazione di trattamento	11. Il trattamento dei dati personali è svolto da un numero indefinito di dipendenti? 12. Qualche parte dell'operazione di trattamento dei dati è svolta da un contraente/terzo? 13. Gli obblighi delle parti/persone

	coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente indicati? 14. Il personale coinvolto nel trattamento dei dati personali non ha familiarità con le questioni di sicurezza informatica? 15. Le persone/parti coinvolte nel trattamento dei dati non si preoccupano di conservare e/o distruggere in modo sicuro i dati personali?
D. Settore di attività e scala del trattamento	16. Consideri il settore di attività come particolarmente esposto ad attacchi informatici? 17. L'organizzazione ha subito attacchi informatici o altre violazioni di sicurezza negli ultimi due anni? 18. Avete ricevuto notifiche e/o reclami riguardanti la sicurezza del sistema IT (utilizzato per il trattamento dei dati personali) nell'ultimo anno? 19. L'operazione di trattamento riguarda un ampio numero di persone e/o di dati personali? 20. Esistono *best practices* di

	sicurezza specifiche per il tuo settore che non sono state adottate?

Seguendo questo approccio, è possibile determinare il livello di probabilità di occorrenza di una minaccia per ciascuna area di valutazione. In altre parole, per ogni dimensione considerata (dalle risorse tecniche e di rete ai processi, dalle persone coinvolte al settore e alla scala del trattamento) si valuta quanto sia realistico che un evento avverso si manifesti. Questo permette di avere una stima più precisa e mirata dei punti di vulnerabilità, facilitando l'identificazione delle aree in cui adottare misure preventive più stringenti e mirate. Per ognuna di queste dimensioni si valuta la probabilità che possa verificarsi un evento avverso, classificandola come bassa, media o alta.

Questa valutazione non si limita a un giudizio qualitativo: a ciascun livello di probabilità viene associato un punteggio numerico, che permette di sommare i valori delle diverse aree e ottenere una stima complessiva della probabilità di occorrenza della minaccia. Il punteggio totale consente quindi di collocare il rischio in una fascia più generale (basso, medio o alto) offrendo un quadro immediatamente interpretabile dell'esposizione complessiva. Questo approccio aiuta a comprendere dove siano più vulnerabili i processi e a guidare le decisioni su quali misure preventive siano necessarie, garantendo che l'attenzione sia concentrata sui punti più critici del trattamento dei dati.

La fase di *Risk Evaluation*, corrispondente allo Step 4 delle linee guida ENISA, costituisce il momento in cui, a partire dal livello di impatto individuato in precedenza e dalla probabilità che l'evento si verifichi, viene determinato il livello complessivo di rischio relativo alla specifica operazione di trattamento.

Tale valutazione presenta una duplice valenza. Da un lato, essa consente di oggettivare il rischio mediante l'applicazione di criteri standardizzati, derivanti dalla combinazione tra la gravità potenziale del

danno e la frequenza stimata delle minacce; dall'altro lato, riconosce al titolare o al responsabile del trattamento un margine di discrezionalità tecnica. Infatti, una volta fornito l'esito della valutazione, è ammesso un intervento correttivo da parte del soggetto obbligato, il quale può modificare il livello di rischio attribuito, purché tale scelta sia accompagnata da un'adeguata motivazione e tenga conto delle peculiarità del contesto di trattamento.

In questo senso, il modello ENISA si colloca a metà strada tra la rigidità di un approccio puramente automatizzato e la flessibilità di una valutazione caso per caso, offrendo al titolare/responsabile uno strumento di supporto decisionale che, tuttavia, non lo esonera dal dovere di documentare e giustificare le proprie scelte in conformità al principio di *accountability* di cui all'art. 5, par. 2, GDPR.

Tabella 5 Livello complessivo di rischio secondo il modello ENISA.

		Danno/livello di impatto		
		Basso	Medio	Alto
Probabilità che l'evento si verifichi	Basso	Rischio basso	Rischio basso	Rischio medio
	Medio	Rischio basso	Rischio medio	Rischio alto
	Alto	Rischio medio	Rischio alto	Rischio molto alto

L'incrocio tra probabilità di accadimento della minaccia (bassa, media, alta) e livello di impatto (basso, medio, alto) determina il livello complessivo di rischio (basso, medio, alto, molto alto).

A seguito della valutazione del livello di rischio, il titolare o il responsabile del trattamento dei dati può procedere alla selezione delle misure di sicurezza idonee alla protezione dei dati personali.

Nella prospettiva della gestione del rischio, alla fase di valutazione deve necessariamente accompagnarsi l'elaborazione di strategie decisionali idonee a governarlo. La qualità della valutazione è strettamente connessa al grado di conoscenza di cui dispone il soggetto valutatore: le conclusioni saranno tanto più attendibili quanto più riusciranno a integrare in modo corretto ed esaustivo l'insieme delle informazioni disponibili. In tale quadro, conoscenza, probabilità e perdite rappresentano le categorie concettuali fondamentali per un approccio conforme allo stato dell'arte in materia di valutazione e gestione dei rischi[319].

Nell'ambito della protezione dei dati personali, un ruolo significativo è svolto dall'Annesso A, dell'*Handbook on Security of Personal Data Processing*[320] dell'ENISA che si concentra sulle misure tecniche e organizzative adottabili. Il documento propone una classificazione che distingue i livelli di rischio in tre gradi – basso, medio e alto – e suggerisce per ciascuno di essi una serie di strumenti di tutela. L'aspetto interessante di questo modello è la logica di progressività che lo sostiene: le misure individuate per il livello più basso costituiscono una sorta di soglia minima, destinata ad applicarsi in ogni caso, anche quando il contesto presenti rischi più consistenti. Se il livello di esposizione cresce, tali misure non vengono sostituite ma integrate da quelle previste per lo scenario intermedio, che a loro volta diventano parte del quadro di riferimento nelle situazioni di rischio elevato. Diversamente, le misure destinate al livello massimo sono concepite come soluzioni straordinarie e rimangono circoscritte ai casi in cui la criticità raggiunga un'intensità tale da richiedere protezioni eccezionali.

Questa impostazione, nel suo insieme, risponde a una duplice esigenza. Da un lato garantisce una protezione che cresce in modo

[319] P. ERTO, M. GIORGIO, I. IERVOLINO, *Probabilità e rischio*, in *Ambiente, rischio, comunicazione-Decidere nell'incertezza*, 2012, 4, 1-11.
[320] ENISA, *Handbook on Security of Personal Data Processing*, 2017.

proporzionato alla gravità del rischio, evitando vuoti di tutela; dall'altro previene l'adozione indiscriminata di misure eccessivamente onerose in contesti che non ne giustificherebbero l'impiego. Ne risulta un sistema dinamico e adattabile, capace di bilanciare sicurezza ed efficienza organizzativa.

In conclusione, da un punto di vista analitico, il rischio può essere definito, nello spazio degli attributi misurabili, come la combinazione tra l'entità del danno o delle conseguenze negative e la probabilità della loro occorrenza. La riduzione del rischio – intesa come incremento del livello di sicurezza – può dunque realizzarsi sia attraverso la diminuzione della gravità delle conseguenze, sia mediante la riduzione della probabilità del loro verificarsi, ovvero congiuntamente attraverso entrambe le dimensioni.

In via convenzionale, la definizione quantitativa di rischio si esprime mediante la formula:

$R = f \times M$

dove f rappresenta la frequenza dell'evento incidentale e M la magnitudo dei suoi effetti, ossia la consistenza delle conseguenze prodotte. La grandezza R, indicata come "indice di rischio", incorpora pertanto in misura equivalente sia il profilo della probabilità che quello della gravità delle conseguenze, offrendo così un parametro sintetico utile alla valutazione e alla gestione giuridica dei rischi[321].

3.4 Valutazione di impatto (Data Protection Impact Assessment)

Il GDPR introduce uno strumento specifico volto a gestire e prevenire i rischi connessi al trattamento dei dati personali: la valutazione d'impatto sulla protezione dei dati o DPIA (Data Protection Impact Assessment). Le DPIA contribuiscono all'obiettivo del Regolamento Generale sulla

[321] S. CANALE, C. FABIANO, S. LEONARDI, *Il concetto di rischio e gli ambiti applicativi dell'analisi del rischio*, *Istituto Strade Ferrovie Aeroporti*, Quaderno n. 100, 1998.

Protezione dei Dati (GDPR) di garantire un elevato livello di tutela dei diritti e delle libertà fondamentali degli individui (in particolare del diritto alla protezione dei dati personali), fungendo sia da misura di responsabilizzazione ex post, utile per dimostrare la conformità al GDPR, sia da meccanismo regolatorio ex ante, che impone ai titolari del trattamento di individuare e affrontare i rischi potenzialmente derivanti dalle operazioni di trattamento previste, nonché l'impatto che tali rischi potrebbero avere sulle persone fisiche[322].

Il regolamento non fornisce una definizione esplicita di DPIA; tuttavia, le "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e sulla determinazione dell'eventuale rischio elevato ai fini del Regolamento (UE) 2016/679*", adottate dal Gruppo di lavoro ex Articolo 29, la descrivono come "*un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire alla gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando tali rischi e individuando le misure adeguate per affrontarli*". Le linee guida sottolineano inoltre che si tratta di uno strumento essenziale per il principio di accountability, in quanto aiuta "*i titolari del trattamento non solo a rispettare i requisiti previsti dal regolamento generale sulla protezione dei dati, ma anche a dimostrare di aver adottato misure adeguate a garantirne l'osservanza*[323]". Il GDPR tratta la Valutazione d'Impatto sulla Protezione dei Dati (DPIA) nell'articolo 35, il quale indica che il titolare del trattamento è tenuto a effettuare la DPIA quando il trattamento è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La DPIA perciò è uno strumento il cui scopo

[322] L. DALLA CORTE, R. VAN BRAKEL, *Data protection impact assessment methods for the urban environment: A report for the Commissie Persoonsgegevens Amsterdam (CPA)*, Tilburg University, 2022, 2-4.
[323] B. BORRILLO, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *Dirittifondamentali.it*, 2020, 2, 326-356.

principale è analizzare sistematicamente, identificare e ridurre al minimo i rischi derivanti dal trattamento dei dati per i diritti degli interessati. In altre parole, si tratta di uno strumento di gestione del rischio che aiuta il titolare a raggiungere e dimostrare la conformità agli obblighi previsti dal GDPR. Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

La differenza principale tra la gestione del rischio "classica" applicata a contesti che non concernono dati personali e la DPIA è che, in quest'ultima, la valutazione del rischio riguarda i diritti degli interessati, e non quelli del titolare. Le linee guida del Gruppo di lavoro ex Articolo 29 individuano diversi criteri che indicano quando un trattamento di dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche. Ne consegue, in base all'articolo 35, che la DPIA è obbligatoria solo in determinati casi[324].

In generale, la valutazione d'impatto è una tecnica di analisi utilizzata per esaminare le possibili conseguenze di un'iniziativa su un interesse o su più interessi rilevanti per la società, qualora tale iniziativa possa costituire una minaccia per questi interessi, con l'obiettivo di sostenere una decisione informata circa l'attuazione dell'iniziativa e le eventuali condizioni da applicare (essa rappresenta, innanzitutto, un mezzo per proteggere tali interessi).

L'obbligo di effettuare la DPIA riflette l'approccio basato sul rischio alla protezione dei dati personali introdotto dal riformato quadro giuridico dell'UE, nonché il rafforzamento del principio di accountability (articolo 5, paragrafo 2 del GDPR). Ispirandosi all'esperienza maturata nell'uso di tecniche valutative in altri ambiti (come le valutazioni d'impatto ambientale, tecnologico o normativo), la DPIA diventa uno strumento efficace per

[324] M. HORÁK, V. STUPKA, M. HUSÁK, *GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform*, in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, 1-8.

garantire il rispetto e l'applicazione della normativa sulla protezione dei dati personali[325].

La condizione giuridica che determina l'obbligo di effettuare una DPIA è il requisito del "rischio elevato". Tale condizione è "costitutiva" nel senso che, se non è probabile che le operazioni di trattamento comportino un rischio elevato per i diritti e le libertà delle persone fisiche, allora non sussiste alcun obbligo giuridico per il titolare del trattamento di eseguire una DPIA. La valutazione d'impatto sulla protezione dei dati rappresenta un adempimento essenziale a carico del titolare del trattamento, da realizzarsi prima dell'avvio delle operazioni di trattamento. Tale valutazione consente di individuare i potenziali rischi per i diritti e le libertà degli interessati e di adottare le misure tecniche e organizzative necessarie per ridurli. Qualora, nonostante le misure adottate, il rischio residuo risulti ancora elevato, il titolare è tenuto a consultare preventivamente l'Autorità di controllo competente, al fine di ottenere indicazioni o autorizzazioni circa la liceità del trattamento previsto.

Il concetto di rischio e il suo significato nel contesto della protezione dei dati ha attirato notevole attenzione da parte dei giuristi. Ciò è giustificato perché, come già illustrato, il rischio rappresenta un criterio fondamentale introdotto affinché le misure siano calibrate e adattate dai titolari del trattamento in base alle specifiche circostanze del trattamento stesso. Nel contesto preso in esame il rischio deve essere valutato nel più ampio contesto dei "diritti e delle libertà degli interessati".

Nel caso della valutazione d'impatto sulla protezione dei dati l'obbligo giuridico sorge solo qualora le operazioni di trattamento risultino verosimilmente suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'aggettivo "elevato" si riferisce a caratteristiche

[325] D. KLOZA et al., *Towards a method for data protection impact assessment*, in *Policy Brief D. Pia. Lab*, 2020, 1, 1-2.

(cioè probabilità elevata e/o gravità elevata) che sono, per definizione, intrinseche alla nozione di rischio. Secondo il Gruppo di lavoro Articolo 29, "*un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità*". Il fatto che si debba tenere conto sia della probabilità che della gravità è ribadito anche nei Considerando 75 e 76 del GDPR.

Pertanto, per giungere alla conclusione che un trattamento possa costituire un rischio (sia esso elevato o meno), il titolare deve prima valutare la gravità del rischio e quanto probabile sia che l'evento si verifichi. Se tale valutazione porta alla conclusione che un rischio elevato è probabile, allora il titolare ha l'obbligo di eseguire una DPIA, con l'obiettivo di mitigare il rischio identificato.

Di conseguenza, non è sufficiente individuare cosa costituisce un rischio per la sicurezza dei dati. È altrettanto fondamentale avere un approccio comune su come il titolare debba valutare la gravità e la probabilità del rischio. Questa triplice valutazione (che riguarda dapprima "che cosa costituisce un rischio", e poi se tale rischio è "elevato" in termini di probabilità e gravità) è una valutazione di un evento ipotetico.

Il legislatore richiede che questa valutazione triplice sia oggettiva. È quindi importante comprendere che cosa significhi "valutazione oggettiva" e in che modo tale oggettività possa essere raggiunta quando i titolari valutano rischi ipotetici, la loro probabilità e la loro gravità. L'obiettivo desiderato è che i titolari effettuino valutazioni del rischio in modo tale che le conclusioni siano affidabili, verificabili, credibili e contestabili. Di conseguenza, è necessario usare un linguaggio e strumenti condivisi da tutti coloro che operano nel campo della protezione dei dati. Detto questo, un informatico e un giurista non condividono la stessa comprensione del concetto di rischio. Pertanto, se un informatico formula un giudizio sul livello di rischio di determinate operazioni di trattamento, un giudice potrebbe avere difficoltà a verificare la fondatezza di tale giudizio e a valutarlo giuridicamente.

Anche se il legislatore non avesse esplicitamente richiesto l'oggettività, questa esigenza emergerebbe comunque implicitamente, vista la scelta dello strumento giuridico del Regolamento (invece di una Direttiva) e il suo obiettivo sottostante di garantire una protezione dei dati armonizzata e di alto livello[326].

Conformemente all'articolo 30(1) del GDPR, i titolari del trattamento devono mantenere un registro di tutte le attività di trattamento svolte sotto la loro responsabilità e, pertanto, tali registri devono contenere determinate informazioni. Sebbene alcune piccole imprese siano esentate da quest'obbligo ai sensi dell'articolo 30(5) del GDPR, il registro delle attività di trattamento deve comunque essere tenuto non appena il trattamento possa comportare dei rischi per i diritti e le libertà degli interessati, oppure riguardi categorie particolari di dati personali ai sensi dell'articolo 9(1) del GDPR. Sarebbe infatti praticamente impossibile svolgere una DPIA (valutazione d'impatto sulla protezione dei dati) senza disporre di queste informazioni di base, che pertanto dovrebbero essere già disponibili all'avvio della DPIA stessa. Il registro dei trattamenti si configura come una vera e propria pietra angolare del sistema di compliance al GDPR, poiché consente di rendere trasparente e verificabile l'intera filiera del trattamento dei dati personali. Attraverso un'adeguata attività di *assessment*, il registro permette di individuare quali dati siano raccolti, per quali finalità vengano utilizzati, da quali unità operative siano gestiti e con quali misure di sicurezza siano protetti, includendo altresì i fornitori e i relativi rapporti contrattuali.

La corretta organizzazione e l'aggiornamento costante del registro agevolano l'elaborazione di procedure interne e la strutturazione di un sistema integrato di gestione della privacy, che non si limita al profilo documentale (nomine, informative, regolamenti), ma si estende anche al piano tecnico e

[326] K. DEMETZOU, *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2019, 35(6).

organizzativo, garantendo chiarezza sui ruoli e sugli strumenti impiegati. In questa prospettiva, il registro non è soltanto un adempimento formale, ma un presupposto operativo imprescindibile, specie per il DPO, il quale fornisce i riferimenti necessari per gestire, entro il termine perentorio di 72 ore, eventuali violazioni dei dati personali (data breach), come previsto dall'art. 33 del GDPR[327].

Le informazioni da fornire nel registro delle attività di trattamento, ai sensi dell'articolo 30(1) del GDPR, includono:

- Nome e dati di contatto del titolare del trattamento, del responsabile (se presente) e del Data Protection Officer (DPO), ove applicabile.
- Finalità del trattamento.
- Descrizione delle categorie di interessati coinvolti nel trattamento.
- Descrizione delle categorie di dati personali oggetto di trattamento.
- Categorie di destinatari cui i dati personali sono stati o saranno comunicati, compresi destinatari in paesi terzi o organizzazioni internazionali.
- Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, con l'indicazione di tale paese o organizzazione e, nel caso dei trasferimenti di cui al secondo comma dell'articolo 49(1) del GDPR, la documentazione delle garanzie adeguate.
- I termini previsti per la cancellazione delle diverse categorie di dati (ove possibile).
- Descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32(1) del GDPR (ove possibile).

Inoltre, è necessario ricordare che, ai sensi dell'articolo 5(1)(a) del GDPR, qualsiasi trattamento di dati personali richiede una base giuridica

[327] A. PIETROLETTI, A. NICOTRA, *Tutela della salute, sistemi digitali e privacy*, in *Rivista Italiana di Informatica e Diritto*, 2022, 4(1), 283-294.

adeguata. Ogni trattamento effettuato senza una valida base giuridica costituisce una violazione del diritto fondamentale alla protezione dei dati personali previsto dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, il che comporta quindi un rischio per i diritti e le libertà degli interessati, nonché una violazione delle norme previste nel GDPR.

Per evitare tali conseguenze, la base giuridica del trattamento previsto deve essere documentata preventivamente.

L'articolo 6(1)(a)-(f) del GDPR elenca sei possibili basi giuridiche per il trattamento dei dati personali. Se vengono trattate categorie particolari di dati personali ai sensi dell'articolo 9(1) del GDPR, o dati relativi a condanne penali e reati conformemente all'articolo 10 del GDPR, è necessario prendere in considerazione anche le ulteriori basi giuridiche previste per tali tipi di dati[328].

Una DPIA può essere richiesta anche nei casi in cui il rischio di un'operazione di trattamento precedentemente classificata come basso sia divenuto elevato, così come nei casi in cui non sia chiaro a quale categoria appartenga una determinata operazione di trattamento.

Nel contesto della Big Data Analytics, i diritti degli interessati da tutelare e i tipi di rischi elevati da evitare non sono del tutto chiari, poiché dipendono solitamente da come viene interpretata la normativa. Di conseguenza, l'ambito di applicazione di una DPIA è stato, in una certa misura, incerto, mentre non esistono requisiti determinati su come un'organizzazione debba condurre una DPIA.

Ad esempio, il riferimento all'uso di nuove tecnologie nell'articolo 35(1) è molto generico e non implica necessariamente la presenza di rischi derivanti dal trattamento dei Big Data. La partecipazione di diversi

[328] N. MARTIN et al., *The Data Protection Impact Assessment According to Article 35 GDPR*, Fraunhofer ISI, Karlsruhe, 2020, 20-21.

stakeholder è sottolineata nell'articolo 35(9), ma senza specificare come debba avvenire tale partecipazione.

Nel tentativo di chiarire meglio quali operazioni di trattamento richiedano una DPIA, autorità di controllo come il Comitato Europeo per la Protezione dei Dati (EDPB) e l'ICO (Information Commissioner's Office della Gran Bretagna), la CNIL (l'Autorità Garante per la protezione dei dati personali francese) hanno pubblicato linee guida (EDPS, 2019[329]; ICO, 2019) e strumenti pratici (Software DPIA, 2015, CNIL) che contengono un elenco non esaustivo di criteri da utilizzare per determinare se un trattamento possa essere considerato ad alto rischio. Le linee guida dell'EDPS sono state ulteriormente perfezionate rispetto a quanto già presentato nel documento WP29, 2017[330] e adottate nella revisione del 4 ottobre 2017[331]. Secondo la versione più recente, nel valutare se le operazioni di trattamento pianificate attivino l'obbligo di effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA), il titolare del trattamento deve utilizzare il modello riportato nell'Allegato 1[332], esposto in coda a questo lavoro, per effettuare una

[329] European Data Protection Supervisor, *Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725*, 2019.

[330] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (WP 248 rev. 01)*, Commissione Europea, 13 ottobre 2017.

[331] G. GEORGIADIS, G. POELS, *Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review*, in *Computer Law & Security Review*, 2022, 44.

[332] Le Linee guida del Gruppo di lavoro Articolo 29 chiariscono che, nei casi dubbi, è comunque raccomandabile effettuare una DPIA come buona prassi di conformità. Vengono inoltre individuati nove criteri principali che aiutano a determinare quando un trattamento presenta un rischio elevato: la valutazione o profilazione degli individui sulla base di dati personali, come punteggi di credito o analisi comportamentali; i processi decisionali automatizzati che producono effetti giuridici o significativi sugli interessati; il monitoraggio sistematico di persone, incluso quello di aree pubbliche o accessibili al pubblico; il trattamento di dati sensibili o altamente personali, come dati sanitari, genetici o relativi a condanne penali; i trattamenti su larga scala, valutati in base al numero di interessati, al volume dei dati e alla durata delle operazioni; la combinazione o interconnessione di insiemi di dati provenienti da fonti diverse; il trattamento di dati di soggetti vulnerabili, quali minori, dipendenti o categorie socialmente svantaggiate; l'uso di nuove tecnologie o soluzioni

valutazione preliminare (*threshold assessment*). L'allegato, sintetizzato, individua una serie di criteri utili per determinare la necessità di effettuare una DPIA, tra cui:

- Trattamenti valutativi o di scoring, inclusa la profilazione;
- Decisioni automatizzate che producono effetti giuridici significativi (ad esempio, assunzioni, concessione di prestiti o stipula di assicurazioni);
- Monitoraggio sistematico (come la videosorveglianza);
- Trattamento di dati sensibili, giudiziari o di natura estremamente personale (ad esempio, opinioni politiche);
- Trattamenti su larga scala di dati personali;
- Combinazione o raffronto di insiemi di dati provenienti da trattamenti distinti o con finalità diverse, anche oltre il consenso iniziale (tipico dei Big Data);
- Dati riferiti a soggetti vulnerabili (minori, persone con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- Utilizzo di tecnologie o soluzioni innovative (come il riconoscimento facciale o dispositivi IoT);
- Trattamenti che possano impedire agli interessati di esercitare un diritto o accedere a un servizio o contratto (ad esempio, screening bancario per la concessione di un finanziamento).

Qualora due o più dei criteri presenti nel modello dell'Allegato 1 risultino applicabili, il titolare del trattamento dovrà, in linea generale, procedere alla realizzazione di una DPIA. Nel caso in cui il titolare del trattamento decida di non effettuare una DPIA, nonostante siano applicabili più di un criterio del modello dell'Allegato 1, dovrà documentare e giustificare tale decisione. Anche nel caso in cui le operazioni di trattamento

innovative, come sistemi biometrici o applicazioni dell'Internet of Things; e infine i trattamenti che limitano l'esercizio di diritti o l'accesso a servizi, ad esempio nel caso di valutazioni creditizie automatizzate.

pianificate attivino un solo criterio del modello dell'Allegato 1, il titolare del trattamento può comunque decidere di effettuare una DPIA[333].

In generale, la presenza contemporanea di due o più di questi criteri indica con elevata probabilità la necessità di effettuare una DPIA. Tale strumento assume quindi una funzione centrale nel garantire un approccio preventivo e responsabile alla tutela dei dati personali, favorendo la trasparenza e la fiducia nei processi di trattamento.

Ai sensi del paragrafo 7 dell'art. 35 del GDPR, la valutazione deve contenere almeno i seguenti elementi fondamentali: i) una descrizione sistematica dei trattamenti previsti e delle relative finalità, comprendendo, ove pertinente, l'indicazione dell'interesse legittimo perseguito dal titolare del trattamento; ii) una valutazione della necessità e della proporzionalità dei trattamenti in relazione alle finalità dichiarate, volta a garantire che i dati personali siano trattati solo nella misura strettamente necessaria per gli scopi perseguiti; iii) una valutazione dei rischi per i diritti e le libertà fondamentali degli interessati, con particolare attenzione alle possibili conseguenze di natura fisica, materiale o immateriale che potrebbero derivare dal trattamento; iv) l'individuazione delle misure previste per affrontare i rischi individuati, incluse le garanzie, le misure di sicurezza tecniche e organizzative, nonché i meccanismi volti ad assicurare la protezione dei dati personali e a dimostrare la conformità ai principi del Regolamento. Tali misure devono tenere conto non solo dei diritti e degli interessi legittimi degli interessati, ma anche di quelli di altre persone eventualmente coinvolte.

In tal modo, la valutazione d'impatto si configura come uno strumento essenziale per l'attuazione del principio di responsabilizzazione

[333] In linea generale, se si applicano due o più criteri dell'elenco, il titolare del trattamento dovrebbe effettuare una DPIA. Se il titolare ritiene che, nel caso specifico, i rischi non siano "elevati" nonostante vi siano più risposte affermative, dovrà spiegare e giustificare perché ritiene che il trattamento non comporti in effetti un rischio elevato.
Ogni criterio è seguito da esempi e controesempi che illustrano quando è probabile o improbabile che venga attivato.

(accountability), consentendo al titolare del trattamento (come indicato all'inizio di questo paragrafo) di dimostrare la conformità al GDPR e di adottare un approccio preventivo e proattivo nella tutela dei dati personali. Un ulteriore elemento di rilievo previsto dall'art. 35, paragrafo 9, del GDPR riguarda la possibilità di coinvolgere gli interessati o i loro rappresentanti nella procedura di valutazione d'impatto sulla protezione dei dati. La norma dispone infatti che, *"se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti"*.

Tale previsione introduce un principio di partecipazione e trasparenza nel processo di valutazione preventiva dei rischi, collocando la DPIA non solo come strumento tecnico di gestione della conformità, ma anche come momento di dialogo tra il titolare e gli interessati. La consultazione, tuttavia, è subordinata a una valutazione di opportunità (*se del caso*) e deve svolgersi in modo tale da non compromettere la riservatezza di informazioni sensibili, né gli interessi economici o di sicurezza collegati al trattamento.

L'Allegato 2 esposto di seguito all'Allegato 1 elenca alcune operazioni comuni di trattamento che, con tutta probabilità, richiedono una DPIA. In tali casi, il titolare del trattamento non è tenuto a svolgere una valutazione preliminare, ma deve procedere direttamente alla realizzazione della DPIA.

Alcune tipologie di trattamenti non richiedono la conduzione di una DPIA poiché considerate a basso rischio per i diritti e le libertà degli interessati. Tra queste rientrano le ordinarie attività amministrative relative alla gestione del personale, come la tenuta dei fascicoli individuali, le procedure standard di selezione e valutazione del personale, la gestione di congedi e flessibilità lavorativa, nonché i sistemi di controllo degli accessi non biometrici e la videosorveglianza su scala limitata, priva di riconoscimento facciale e confinata agli spazi interni. Tali operazioni, di

natura routinaria e proporzionata, non comportano un rischio elevato tale da giustificare una DPIA preventiva e sono riportati più nel dettaglio nell'Allegato 3.

La DPIA rappresenta dunque un processo iterativo di governance del rischio articolato in tre fasi. In primo luogo, l'organizzazione identifica le proprie attività di trattamento dei dati. Successivamente, verifica se tali attività soddisfano uno o più criteri che rendono necessaria la conduzione di una DPIA. Qualora tali criteri risultino soddisfatti, l'organizzazione è tenuta a svolgere una DPIA[334]. In base alle linee guida dell'EDPS, qualora la valutazione d'impatto sulla protezione dei dati evidenzi la persistenza di rischi residui elevati per i diritti e le libertà degli interessati, il titolare del trattamento è tenuto a richiedere una consultazione preventiva dell'autorità di controllo, come previsto dall'articolo 36, paragrafo 1 del GDPR. In tale fase, la DPIA deve essere presentata nella sua versione completa (articolo 36, paragrafo 3, lettera e), in modo da consentire all'autorità una valutazione accurata delle misure adottate e dei rischi ancora presenti. L'autorità potrà esprimere un parere, assicurando tuttavia la tutela di eventuali segreti commerciali e la non divulgazione di informazioni sensibili relative alla sicurezza, nel rispetto delle normative nazionali che disciplinano l'accesso ai documenti ufficiali.

La seguenti figure, come elaborato dalle linee guida del Gruppo di Lavoro ex Articolo 29 schematizzano i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati e al processo iterativo generico per lo svolgimento di una DPIA:

[334] Secondo l'EDPS, la "*La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93)23. Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78). La valutazione d'impatto sulla protezione dei dati va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento".*

Figura 1 Principi fondamentali relativi alla DPIA.

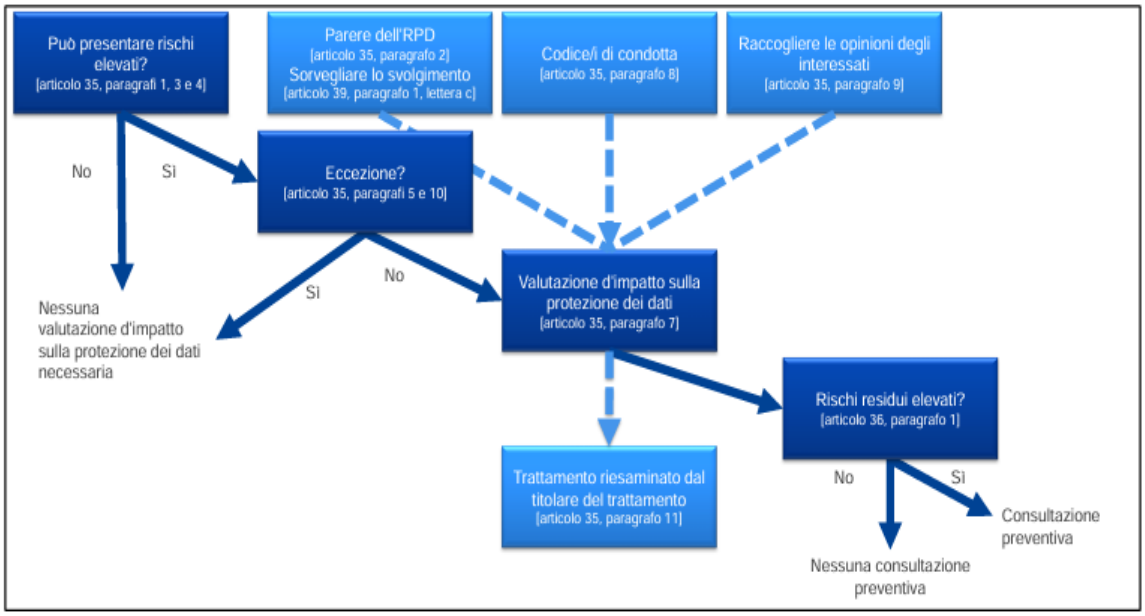
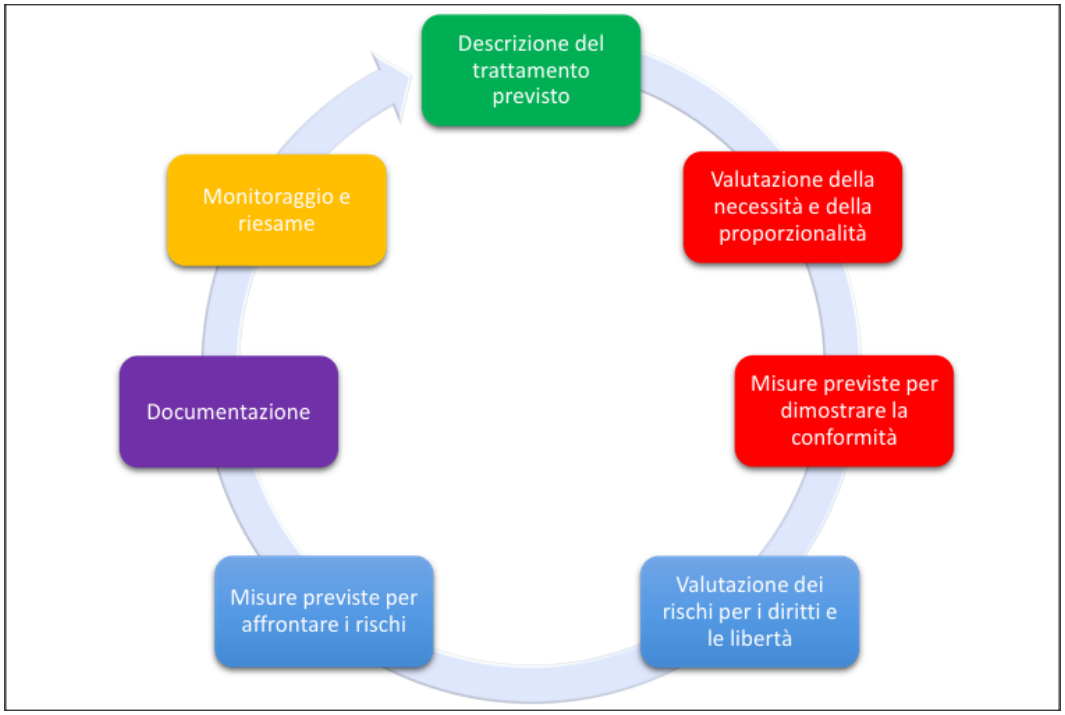


Figura 2 Fasi del processo iterativo generico per lo svolgimento di una DPIA.



Come già sottolineato il GDPR non impone un metodo rigido per l'esecuzione delle valutazioni dei rischi e degli impatti, ma si limita a stabilire requisiti generali. In tale contesto, le Autorità Garanti per la Protezione dei Dati (Data Protection Authorities), responsabili dell'attuazione del GDPR, hanno pubblicato, attraverso i propri siti istituzionali, linee guida e strumenti a supporto della conformità normativa, con particolare riferimento alla DPIA e ai meccanismi di governance del rischio. La CNIL, Autorità francese per la protezione dei dati personali, ha sviluppato uno strumento denominato PIA (Privacy Impact Assessment), volto a supportare le organizzazioni nella documentazione, revisione e condivisione delle informazioni relative alle DPIA. Tale strumento è open source, gratuito e può essere utilizzato sia come software autonomo, sia installato su un server (ad esempio, per favorire la condivisione dei dati all'interno di un'organizzazione)[335].

Sebbene i titolari del trattamento siano liberi di adottare una delle metodologie esistenti per la valutazione d'impatto sulla protezione dei dati – come quelle raccomandate dal Garante europeo della protezione dei dati (EDPS)[336] – o di svilupparne una propria, affinché tale processo risulti realmente efficace, esso dovrebbe includere almeno i seguenti elementi:

- Una chiara definizione dei ruoli e delle responsabilità delle diverse figure coinvolte nel processo di DPIA, specificando, ad esempio, chi sarà incaricato della valutazione dei rischi, chi selezionerà le misure di mitigazione e chi approverà il rapporto finale. In presenza di contraenti esterni, è necessario descrivere il loro ruolo e le interazioni con i principali stakeholder del sistema.

[335] H. J. PANDIT et al., T*owards a Semantic Specification for GDPR Data Breach Reporting*, in *Frontiers in Artificial Intelligence and Applications*, vol. 379, IOS Press, 131-136.
[336] European Data Protection Supervisor, *EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation*, 2020.

- Una modalità strutturata per descrivere i processi aziendali e i flussi di dati, utile a contestualizzare il trattamento e a visualizzare i punti critici sotto il profilo della protezione dei dati.
- Un metodo per identificare gli eventi che potrebbero generare rischi per i diritti e le libertà degli interessati.
- Una tecnica per stimare la probabilità e l'impatto di tali eventi.
- Un sistema per calcolare il rischio complessivo per gli interessati, combinando la probabilità, l'impatto e la natura degli eventi individuati.
- Indicazioni sui criteri decisionali utilizzati dal management del titolare del trattamento per determinare quali rischi mitigare e attraverso quali opzioni.
- Una metodologia per proporre e giustificare le misure di mitigazione da implementare al fine di ridurre i rischi per gli interessati;
- Un metodo per calcolare i rischi residui che permangono dopo l'attuazione delle misure di mitigazione.
- Elementi esplicativi su come il management gestirà i rischi residui, comprese le strategie decisionali e le alternative disponibili.

In conclusione, l'analisi dei rischi condotta nell'ambito della DPIA è, nella maggior parte dei casi, di tipo qualitativo, basata su scale di valutazione che stimano separatamente la probabilità degli eventi, il loro impatto e il livello complessivo di rischio.

3.5 Data Breach e Severity Calculator

Quando informazioni riservate vengono sottratte, visualizzate o sfruttate senza autorizzazione, l'evento viene solitamente indicato come una "violazione dei dati" (data breach). Il termine 'dato' può avere significati diversi a seconda del contesto, ma i dati considerati 'sensibili' necessitano normalmente di una protezione più stringente.

Come supportato dalle analisi di M. Iaselli, il concetto di 'distruzione' dei dati personali è abbastanza intuitivo: si parla di distruzione quando i dati non esistono più o non sono più disponibili in una forma utile per il titolare del trattamento. Anche il termine 'danno' è relativamente chiaro: si verifica quando i dati personali sono stati alterati, corrotti o risultano incompleti. Per "perdita" dei dati personali si intende invece la situazione in cui i dati potrebbero ancora esistere, ma il titolare del trattamento ha perso il controllo o l'accesso agli stessi, oppure non li possiede più. Infine, un trattamento non autorizzato o illecito comprende la divulgazione di dati personali a soggetti non autorizzati o l'accesso da parte di destinatari non autorizzati, così come qualsiasi altra modalità di trattamento che violi le disposizioni del regolamento. Va sottolineato che, anche se una temporanea indisponibilità dei sistemi del titolare del trattamento potrebbe non avere effetti diretti sugli individui, è fondamentale che il titolare valuti tutte le possibili conseguenze della violazione, poiché potrebbe comunque essere necessario segnalarla per altri motivi. Una violazione dei dati può infatti comportare numerosi effetti negativi significativi sulle persone fisiche, con danni di natura fisica, materiale o immateriale[337].

Le conseguenze che possono scaturire dalle violazioni dei dati sono molteplici e sono influenzate da fattori quali il tipo di dati compromessi, le cause alla radice degli incidenti e la tempestività della risposta. Nell'era digitale, le violazioni dei dati sono diventate una preoccupazione crescente, comportando rischi significativi sia per le organizzazioni che per gli individui. La proliferazione di dati non strutturati provenienti da piattaforme di condivisione online, canali social e servizi cloud ha aumentato l'esposizione di informazioni sensibili, rendendo la protezione dei dati più

[337] M. IASELLI, *Guida alla nuova procedura di data breach*, Milano, Giuffrè Francis Lefebvre, 2021, 5-8.

critica che mai[338]. Per gli interessati, l'accesso non autorizzato ai propri dati personali, come codici fiscali, date di nascita e indirizzi, può comportare il furto d'identità e rischi per la propria incolumità fisica[339]. A seconda della tipologia di dati archiviati, possono sorgere ulteriori problematiche, ad esempio la diffusione di informazioni sulle carte di credito che favorisce frodi finanziarie, oppure la violazione delle cartelle cliniche con la conseguente esposizione di diagnosi sensibili.

Analogamente, per le imprese e per le amministrazioni pubbliche, la divulgazione non intenzionale di dati può determinare rilevanti pregiudizi, quali il danno reputazionale, conseguenze legali e perdite economiche. Per tali ragioni, tanto i soggetti privati quanto quelli pubblici sono tenuti a predisporre idonei presidi di sicurezza, volti a prevenire accessi non autorizzati, violazioni o utilizzi indebiti delle informazioni sensibili. L'adozione di misure tecniche e organizzative robuste, quali la crittografia, i sistemi di controllo degli accessi e le verifiche periodiche di sicurezza, costituisce elemento chiave per garantire la protezione dei dati aziendali e, al contempo, la tutela della riservatezza degli interessati[340]. Due casi emblematici di grande risonanza in questo contesto sono stati la violazione dei dati di Equifax[341] nel 2017 e lo scandalo di Cambridge Analytica,

---

[338] C. GILBERT, M.A. GILBERT, *Impact of General Data Protection Regulation (GDPR) on Data Breach Response Strategies (DBRS)*, in *International Journal of Research and Innovation in Social Science*, 2025, 9(14), 760-784.

[339] La violazione della privacy non costituisce l'unica problematica derivante da un uso inconsapevole o fraudolento delle nuove tecnologie. Emergono, infatti, ulteriori rischi significativi per l'individuo, tra cui minacce alla sicurezza pubblica e privata, la diffusione e condivisione non controllata di dati personali, il cyberbullismo, la produzione e diffusione di deepfake e fake news, nonché altri abusi online. Su tali fenomeni, l'Autorità per le comunicazioni ha da tempo avviato specifici approfondimenti e iniziative di monitoraggio. A. ALONGI, F. POMPEI, *Diritto della privacy e protezione dei dati personali – Il GDPR alla prova della data driven economy*, Roma, Tab Edizioni, 2021, 13-15.

[340] G.A. PIMENTA RODRIGUES et al., *Understanding data breach from a global perspective: Incident visualization and data protection law review*, in *Data*, 2024, 9(2), 1-2.

[341] Equifax Inc., con sede ad Atlanta, Georgia, è una multinazionale statunitense attiva nel settore dei servizi di informazione creditizia ed è considerata, insieme a Experian e TransUnion, una delle tre principali agenzie mondiali di credit reporting. Nel settembre 2017 l'azienda ha reso noto di aver subito una grave violazione informatica che ha compromesso i dati personali di circa 147 milioni di individui. Per affrontare le conseguenze dell'incidente,

connesso alla raccolta e diffusione non autorizzata di informazioni degli utenti di Facebook. Eventi di questa portata hanno avuto un impatto a livello globale e sottolineano l'urgenza di garantire la sicurezza dei dati sia per i consumatori, sia per le organizzazioni che li custodiscono, sia per gli stati che intendono proteggere i propri cittadini. Il primo obbligo nell'Unione Europea relativo alla notifica delle violazioni di dati è stato introdotto con la Direttiva ePrivacy (2009/136/CE), emanata nel 2002 e successivamente aggiornata nel 2009. Tale normativa descriveva la violazione di dati personali come "*qualsiasi compromissione della sicurezza che provochi accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali".* Essa imponeva inoltre che *"il fornitore… informi gli utenti… e notifichi senza ritardi ingiustificati l'accaduto all'autorità nazionale competente*".

In combinazione con la Direttiva sulla protezione dei dati (DPD), la Direttiva ePrivacy costituì la base del sistema europeo di tutela della privacy e di gestione dei dati. I singoli Stati membri, tuttavia, aggiunsero regole proprie, sia di carattere generale sia specifiche per determinati settori, generando difformità normative tra i diversi ordinamenti. Proprio queste differenze spinsero verso un approccio più uniforme, culminato con l'adozione del Regolamento generale sulla protezione dei dati (GDPR)[342].

Il GDPR, superando la precedente tendenza a circoscrivere la sicurezza a un profilo meramente tecnico-operativo, eleva la stessa a principio cardine del trattamento dei dati personali, riconoscendole una funzione essenziale nella tutela dei diritti e delle libertà fondamentali degli interessati. Ne deriva l'esigenza di adottare strumenti tecnici e organizzativi

Equifax ha raggiunto un accordo con la Federal Trade Commission, il Consumer Financial Protection Bureau e con 50 stati e territori degli Stati Uniti, stanziando fino a 425 milioni di dollari a favore delle persone colpite.

[342] J. NIELD, J. SCANLAN, E. ROEHRER, *Exploring consumer information-security awareness and preparedness of data-breach events*, in *Library Trends*, 2020, 68(4), 611-635.

costantemente aggiornati e adeguati, in grado di ridurre al minimo i rischi e di garantire una risposta immediata in caso di violazione dei dati personali[343].

Un incidente di violazione dei dati inizia quando la violazione è sospettata o rilevata e termina con la stesura di un rapporto finale che ne dettaglia gli impatti e le misure di mitigazione adottate. Oltre a queste fasi, i processi organizzativi possono includere fasi in cui le informazioni disponibili al riguardo sono poco chiare o ambigue, ad esempio quando non sono disponibili dati sufficienti per stabilire con certezza l'esistenza di una violazione, oppure quando una violazione è solo sospettata ma non ancora confermata[344]. L'Articolo 4, paragrafo 12 del GDPR, definisce una violazione dei dati personali come "*una compromissione della sicurezza che comporti la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, archiviati o comunque trattati, in modo accidentale o illecito*". La definizione si concentra quindi sulle conseguenze della violazione, ovvero la possibile perdita di riservatezza, integrità e disponibilità dei dati personali. Eventuali differenze legate all'origine della violazione, ad esempio se essa sia intenzionale o derivante da negligenza, non sono rilevanti ai fini della definizione.

L'Articolo 33, stabilisce quali soggetti siano tenuti a notificare le violazioni dei dati, ovvero i "titolari del trattamento" che possono essere persone fisiche, giuridiche o autorità pubbliche, in tal modo, l'obbligo di notificare il data breach si rende applicabile sia alle organizzazioni private sia a quelle pubbliche. La nomina di un Data Protection Officer (DPO), insieme al mantenimento di un registro dei trattamenti costantemente aggiornato e a una gestione corretta di eventuali violazioni dei dati (esfiltrazioni o accessi

[343] M. RENNA, *La disciplina del data breach nel GDPR: note su violazione dei dati personali e sicurezza del trattamento*, in *Actualidad jurídica iberoamericana*, 2023, 18, 992-1007.
[344] H. J. PANDIT et al., *Towards a Semantic Specification for GDPR Data Breach Reporting*, in *Frontiers in Artificial Intelligence and Applications*, vol. 379, IOS Press, 131-136.

non autorizzati agli archivi aziendali), è considerata da molti come uno dei primi e più urgenti adempimenti da attuare per garantire un approccio efficace alla sicurezza dei dati. L'obbligo di mantenere un registro delle violazioni è strettamente legato al principio di responsabilizzazione (accountability) del GDPR, secondo cui i titolari sono responsabili della conformità al regolamento e devono essere in grado di dimostrarla[345]. Da un lato, il principio di accountability offre a titolari e responsabili maggiore libertà nella scelta delle misure di sicurezza e delle politiche di protezione dei dati, senza vincoli rigidi. Dall'altro, però, l'inosservanza o l'adeguamento incompleto comporta conseguenze economiche estremamente rilevanti, le più gravose mai previste nel settore.

L'Articolo 2, paragrafo 2, esclude dall'obbligo di notifica alcune tipologie di violazioni: dati che (a) ricadono al di fuori del campo di applicazione del diritto UE; (b) rientrano nell'ambito del Capo 2 del Titolo V del TUE; (c) siano trattati da persone fisiche per uso personale; o (d) siano utilizzati per l'esercizio di attività di accertamento penale.

Gli Articoli 33 e 34 regolano l'obbligo effettivo di comunicare una violazione. Vi è una differenza apparente tra la notifica a un'autorità di protezione dei dati (DPA, Articolo 33) e la comunicazione agli interessati (Articolo 34). Per quanto riguarda la DPA, il titolare del trattamento deve notificare l'evento "salvo che sia improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche". Tale "probabilità" rappresenta quindi la soglia chiave per l'obbligo di notifica. L'Articolo 33, al paragrafo 1, specifica inoltre che la notifica deve essere effettuata "senza ingiustificato ritardo e, ove possibile, entro 72 ore" dall'accaduto; tuttavia, qualora ciò non sia fattibile, l'organizzazione può notificare più tardi, indicando le ragioni del ritardo. Ai sensi del paragrafo 3 dello stesso articolo,

[345] C.C. ROMITO, *Il GDPR nella micro, piccola e media impresa*, Milano, Giuffré, 2021, 131-132.

il titolare deve includere informazioni sulla natura della violazione, le conseguenze per gli interessati, le contromisure adottate e un punto di contatto. Quando possibile, dovrebbero essere indicati anche il tipo e il numero degli interessati coinvolti e il volume dei dati compromessi.

L'Articolo 34 stabilisce che la soglia per notificare obbligatoriamente gli interessati sia più alta rispetto a quella richiesta per le DPA. La notifica agli interessati è obbligatoria solo quando la violazione "è suscettibile di comportare un rischio elevato per i diritti e le libertà" delle persone coinvolte. Inoltre, la tempistica non è vincolata alle 72 ore dell'Articolo 33, ma deve avvenire "senza ingiustificato ritardo". Non è necessario descrivere la natura della violazione né il numero di interessati coinvolti. L'Articolo 34, paragrafo 3, prevede tre possibili motivi per non comunicare agli interessati: dati resi difficilmente utilizzabili (ad esempio tramite crittografia), misure successive che eliminano il rischio elevato, o onere sproporzionato per l'organizzazione. L'Articolo 34, paragrafo 4, consente alla DPA di richiedere comunque una notifica agli interessati se valuta che il rischio di conseguenze negative sia 'elevato'.

L'Articolo 83, paragrafo 4, prevede sanzioni fino a 10 milioni di euro o al 2% del fatturato annuo dell'impresa, a seconda del valore maggiore, in caso di mancata notifica[346].

Come sostenuto dagli autori Borgesius et al.[347], uno dei motivi alla base dell'obbligo di notifica delle violazioni è permettere alle persone di proteggersi dopo essere state informate. Come afferma il considerando 86 del GDPR, il titolare del trattamento dovrebbe notificare le violazioni ad alto rischio al soggetto interessato "per consentirgli di adottare le necessarie precauzioni".

[346] B. NIEUWESTEEG, M. FAURE, *An analysis of the effectiveness of the EU data breach notification obligation*, in *Computer Law & Security Review*, 2018, 34(6), 1232-1246.
[347] F.Z. BORGESIUS et al., *The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects*, in *SCRIPTed*, 2023, 20, 352-381.

In alcuni casi, tale obbligo può effettivamente essere utile. Ad esempio, gli interessati possono cambiare le proprie password se vengono informate di una fuga di dati contenente le loro credenziali, oppure bloccare la propria carta di credito dopo una violazione che coinvolge informazioni bancarie.

Tuttavia, ci sono diverse questioni da considerare:

- Alcuni dati personali sono difficili o impossibili da modificare. Ad esempio, i dati sanitari contengono informazioni sensibili e ad alto rischio, ma la possibilità di intervenire direttamente è limitata, anche se la fuga di dati è nota.
- L'obbligo di notifica, pur essendo importante, sposta la responsabilità della protezione dal titolare al soggetto interessato.
- Esistono dubbi sull'efficacia di affidare la protezione dei dati al soggetto stesso, perché spesso gli interessati non possiedono le competenze tecniche necessarie per difendersi adeguatamente da furti d'identità o altri rischi collegati alla violazione dei dati.

Si ricorda inoltre che le decisioni adottate dall'autorità di controllo possono essere impugnate mediante ricorso, esperibile anche in caso di inerzia della stessa, di ritardi nella trattazione o nelle informazioni da fornire all'interessato (art. 78). Accanto a tale sistema di tutela di matrice pubblicistica, il GDPR ha previsto strumenti e rimedi di natura privatistica, volti a colmare eventuali insufficienze del public enforcement. All'interessato, in particolare, l'art. 79, par. 1, del regolamento riconosce, in attuazione dell'art. 47 della Carta, la possibilità di proporre un'azione nei confronti del titolare (o del responsabile) del trattamento dinanzi a un'autorità giudiziaria, qualora ritenga che i diritti conferitigli dal regolamento siano stati violati in seguito a un trattamento. Poiché il rispetto di tali diritti da parte del titolare (o del responsabile) implica l'adempimento di specifici obblighi di facere o di non facere, ne deriva che l'azione in questione sarà ordinariamente finalizzata a ottenere un provvedimento inibitorio. Di gran rilievo risulta

anche la tutela risarcitoria disciplinata dall'art. 82: la disposizione, che ha sin da subito attirato l'attenzione di numerosi commentatori, attribuisce infatti a "chiunque" abbia subito un danno "materiale o immateriale" derivante da una violazione del regolamento "il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento[348]".

Per evitare di incorrere in sanzioni, tra le diverse misure possibili in ambito informatico, le autorità di controllo richiedono in particolare l'adozione di strumenti di auditing, e più nello specifico di attività come *vulnerability scan* e *penetration test.*

Per quanto riguarda invece il requisito di dimostrare l'adeguatezza delle misure adottate, il vantaggio dei sistemi e dei programmi informatici consiste nel fatto che, per impostazione predefinita, essi producono (o possono produrre) una grande quantità di informazioni relative al loro funzionamento, i cosiddetti log. Di conseguenza, il comportamento richiesto al titolare è quello di configurare e conservare in maniera corretta tali messaggi di log. La gestione degli accessi rappresenta uno degli ambiti nei quali le autorità di controllo riscontrano più frequentemente violazioni delle misure di sicurezza. Tale presidio non si limita alla dimensione tecnica, ma assume una rilevanza essenzialmente organizzativa, poiché definisce chi, all'interno o all'esterno di un'organizzazione, può accedere a determinati dati, inclusi quelli personali. Una corretta gestione degli accessi consente di circoscrivere l'accesso ai soli soggetti che ne abbiano effettiva necessità per lo svolgimento delle proprie funzioni, riducendo il rischio di trattamenti illeciti.

Questo principio si applica sia agli utenti interni (dipendenti, collaboratori o consulenti), sia a soggetti esterni (fornitori, clienti o visitatori),

[348] F. RAGNO, *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR*, in *Ordine internazionale e diritti umani*, 2020, 4, 818-838.

richiedendo procedure in grado di garantire un controllo puntuale e costante degli accessi.

Un elemento centrale è l'autenticazione degli utenti. Ogni utente deve disporre di un account individuale, soprattutto se ricopre ruoli di responsabilità, così da rendere possibile l'attribuzione certa delle azioni compiute e garantire il principio di accountability previsto dal GDPR. La condivisione delle credenziali costituisce invece una violazione delle misure di sicurezza, compromettendo il controllo sull'operato dei soggetti autorizzati. In ogni caso, l'assegnazione di account individuali o l'autenticazione di un utente costituisce soltanto la misura di sicurezza iniziale. Tale passaggio deve necessariamente essere seguito dalla definizione delle categorie di dati cui ciascun account può accedere, e, di conseguenza, dall'assegnazione delle relative autorizzazioni. Una delle categorie di vulnerabilità maggiormente segnalate dalle autorità di controllo riguarda l'uso di applicazioni non aggiornate o obsolete. È frequente che, successivamente al rilascio di un'applicazione, vengano identificate vulnerabilità che ne compromettono la sicurezza. In tali circostanze, gli sviluppatori rilasciano generalmente aggiornamenti volti a correggere le falle individuate. Tuttavia, qualora tali aggiornamenti non vengano installati tempestivamente, il sistema rimane esposto a rischi significativi, non solo per la presenza della vulnerabilità stessa, ma soprattutto perché questa diventa di dominio pubblico e, di conseguenza, facilmente sfruttabile da un numero potenzialmente elevato di soggetti malintenzionati.

Una delle categorie di vulnerabilità più frequentemente rilevate dalle autorità di controllo riguarda la sicurezza dei dati, in particolare per quanto attiene alle modalità di conservazione e di condivisione. Sebbene esista una vasta gamma di misure tecniche e organizzative finalizzate a proteggere i dati (tra cui la pseudonimizzazione o la cifratura, espressamente richiamate dall'articolo 32, paragrafo 1, lettera a) del GDPR) per ragioni di natura pratica

o tecnica[349] non sempre è possibile implementarle pienamente o garantire il livello massimo di sicurezza[350].

In aggiunta, secondo l'ENISA[351], la quale monitora costantemente il panorama delle minacce informatiche e ne verifica lo stato attraverso il suo rapporto annuale ENISA Threat Landscape (ETL), la segmentazione rappresenta uno dei metodi più efficaci per ridurre la propagazione interna durante un attacco informatico. Le reti dovrebbero essere anche micro-segmentate. Suddividendo una rete in sezioni più piccole e isolate, si impedisce agli attaccanti che riescano a penetrare in un segmento di muoversi liberamente all'interno dell'intero sistema.

Il rapporto ENISA identifica numerose minacce informatiche, evidenziando come le minacce rivolte alla disponibilità dei sistemi occupino la posizione di maggiore rilevanza, seguite da attacchi di tipo ransomware e minacce ai dati. L'analisi condotta dal rapporto si basa su diverse migliaia di incidenti ed eventi di cybersecurity resi pubblici, offrendo un

[349] Un ulteriore nodo critico riguarda la possibilità di ricavare dati personali a partire da informazioni che, almeno in un primo momento, non avevano quella qualificazione. L'esperienza dimostra come, attraverso l'impiego delle tecniche di analisi dei Big Data, sia spesso possibile risalire a profili individuali e a dettagli sensibili partendo da tracce apparentemente neutre. A ciò si aggiunge il problema degli accessi abusivi a banche dati che, grazie a procedure di de-pseudonimizzazione, rendono nuovamente identificabili dati che erano stati resi anonimi solo in via provvisoria. Non meno complessa è la questione legata all'impiego dei sistemi di intelligenza artificiale, i quali, nello svolgimento delle funzioni loro affidate, finiscono talvolta per trattare informazioni personali, con implicazioni significative per la tutela della riservatezza e dei diritti fondamentali. G. BELLOMO, *Contributo alla problematica della natura giuridica del "Data Protection Officer" (DPO)*, in *Consulta Online*, numero speciale *"Liber Amicorum per Pasquale Costanzo"*, 26 marzo 2020, 219-237.

[350] J.S. VANEGAS, *La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR*, in *Rivista italiana di informatica e diritto*, 2020, 2(2), 5-14.

[351] Dal punto di vista tecnico, un ruolo di primaria importanza nel supportare gli operatori nella definizione e nell'attuazione delle misure di sicurezza è svolto dall'ENISA (European Union Agency for Cybersecurity). Tale agenzia, istituita per promuovere un livello elevato e uniforme di sicurezza informatica all'interno dell'Unione europea, rappresenta oggi un punto di riferimento imprescindibile sia per le istituzioni pubbliche sia per gli operatori privati. Le linee guida, i report e le raccomandazioni dell'ENISA forniscono, infatti, strumenti operativi e standard condivisi che consentono di tradurre i principi normativi, sanciti dal GDPR e dalla normativa europea in materia di cybersecurity, in pratiche concrete ed efficaci di prevenzione e protezione. A. PIETROLETTI, A. NICOTRA, *Tutela della salute, sistemi digitali e privacy*, in *Rivista italiana di informatica e diritto*, 2022, 4(1), 283-294.

approfondimento dettagliato sulle principali categorie di minaccia. Tra queste si annoverano: il ransomware e il malware, le tecniche di social engineering, le minacce rivolte ai dati, gli attacchi volti a compromettere la disponibilità dei sistemi come i Denial of Service, le forme di manipolazione e interferenza delle informazioni e, infine, gli attacchi alla catena di approvvigionamento (*supply chain attacks*). Questo quadro consente di comprendere non solo la frequenza e la gravità di tali minacce, ma anche le aree critiche su cui concentrare gli interventi di mitigazione e le strategie di difesa[352].

In tale contesto, le Autorità di protezione dei dati di Grecia e Germania, in collaborazione con l'ENISA hanno elaborato una metodologia volta alla valutazione della gravità delle violazioni dei dati personali (data breach severity calculator), destinata ad essere utilizzata sia dalle stesse Autorità di controllo sia dai titolari del trattamento[353].

La metodologia proposta intende offrire ai titolari del trattamento uno strumento pratico, anche quantitativo, per valutare la gravità delle violazioni di dati personali. Ciò consente di adempiere agli obblighi di notifica all'Autorità (art. 33 GDPR) e di comunicazione agli interessati (art. 34 GDPR), oltre che di individuare misure di mitigazione adeguate. Parallelamente, lo stesso strumento fornisce alle Autorità competenti un criterio uniforme di valutazione, utile per analisi statistiche e per favorire l'armonizzazione a livello europeo, in particolare nei casi di violazioni transfrontaliere.

Ai fini della presente metodologia, la gravità di una violazione di dati personali è definita come la "stima dell'entità del potenziale impatto sugli interessati derivante dalla violazione".

---

[352] ENISA. (2024). *ENISA Threat Landscape 2024*. Agenzia dell'Unione Europea per la Cybersicurezza.

[353] ENISA. (2013). *Recommendations for a methodology for the assessment of severity of personal data breaches*. Agenzia dell'Unione Europea per la Cybersicurezza.

L'utilizzo della metodologia guida il titolare del trattamento attraverso criteri quantitativi specifici, finalizzati a effettuare una valutazione complessiva della gravità della violazione. Gli stessi criteri possono essere adottati dalle Autorità competenti, integrandoli con le informazioni fornite dal titolare nella notifica, per pervenire a una propria valutazione indipendente.

Si osserva tuttavia che il titolare applica la metodologia sulla base delle informazioni disponibili al momento della violazione. Per tale motivo, la metodologia non può necessariamente considerare tutti i possibili scenari, comprese le ricadute su gruppi specifici di soggetti o casi particolarmente complessi che non possono essere pienamente affrontati attraverso un approccio generale. Di conseguenza, sia i titolari del trattamento sia le Autorità competenti devono prestare particolare attenzione nei casi che, per le loro specificità, richiedono una valutazione più approfondita e non completamente coperta dalla metodologia standard.

Nell'ambito della metodologia proposta, la gravità di una violazione di dati personali viene valutata sulla base di tre criteri principali:

- Data Processing Context (DPC – Contesto del trattamento dei dati): prende in considerazione il tipo di dati coinvolti e fattori relativi al contesto complessivo del trattamento.
- Ease of Identification (EI – Facilità di identificazione): valuta quanto facilmente l'identità degli interessati può essere ricavata dai dati oggetto della violazione.
- Circumstances of Breach (CB – Circostanze della violazione): riguarda le modalità della violazione, comprese la perdita di sicurezza dei dati e l'eventuale presenza di intenzionalità dolosa o illecita.

Sulla base dei criteri sopra descritti, l'approccio metodologico adottato può essere sintetizzato come segue. Il Data Processing Context (DPC – Contesto del trattamento dei dati) costituisce il nucleo della metodologia, poiché valuta la criticità di un determinato insieme di dati all'interno del

contesto specifico del trattamento. L'Ease of Identification (EI – Facilità di identificazione) agisce come fattore correttivo del DPC: l'indice complessivo di criticità del trattamento può infatti essere ridotto in funzione del valore di EI, in quanto una minore facilità di identificazione degli interessati comporta un punteggio globale inferiore. La combinazione di DPC ed EI, mediante moltiplicazione, determina il punteggio iniziale di gravità (Severity – SE) della violazione. Il criterio relativo alle Circumstances of Breach (CB – Circostanze della violazione) quantifica invece fattori specifici che possono o meno presentarsi in una data situazione. Quando tali circostanze sono presenti, esse possono soltanto aumentare la gravità della violazione; di conseguenza, il punteggio iniziale viene ulteriormente corretto in funzione del CB.

Il punteggio finale della valutazione della gravità può essere determinato mediante la formula prevista dalla metodologia:

$$SE = DPC \times EI + CB$$

Per determinare il punteggio relativo al Data Processing Context (DPC – Contesto del trattamento dei dati), il titolare del trattamento deve innanzitutto identificare le tipologie di dati personali coinvolti nella violazione e classificarle in almeno una delle quattro categorie previste dalla metodologia: dati semplici, dati comportamentali, dati finanziari e dati sensibili. Questo passaggio consente di ottenere un punteggio preliminare di base. Sebbene l'elenco delle categorie non sia esaustivo, nella maggior parte dei casi concreti i dati possono essere ricondotti ad almeno una delle categorie indicate; le credenziali di accesso, in quanto tali, non costituiscono una categoria autonoma e devono essere valutate in funzione del tipo di dati a cui consentono l'accesso. Successivamente, il punteggio preliminare viene corretto alla luce di fattori contestuali legati al trattamento, quali il volume dei dati, caratteristiche specifiche del titolare o degli interessati, incompletezza o inesattezza dei dati, disponibilità pubblica precedente alla violazione e natura dei dati stessi. In presenza di tali fattori, il punteggio di

base deve essere aumentato o ridotto secondo le scale di aggiustamento previste dalla metodologia, che includono esempi di casi concreti in cui le caratteristiche dei dati o del contesto possono comportare punteggi più elevati o più bassi.

L'Ease of Identification (EI – Facilità di identificazione) misura quanto sia semplice, per una parte in possesso del set di dati, collegare in modo univoco le informazioni a un determinato individuo. Ai fini della metodologia, sono stati definiti quattro livelli di EI – trascurabile, limitata, significativa e massima – con incremento lineare del punteggio. Il livello più basso corrisponde a una possibilità di identificazione trascurabile, ossia quando è estremamente difficile associare i dati a una persona specifica, pur restando possibile in determinate condizioni. Il livello massimo si applica quando l'identificazione può avvenire direttamente dai dati compromessi, senza alcuna ricerca aggiuntiva. La determinazione di EI deve considerare sia le modalità dirette (ad esempio tramite nome) sia quelle indirette (ad esempio tramite numero identificativo) di identificazione, nonché il contesto specifico della violazione, poiché gli stessi identificatori possono comportare punteggi differenti a seconda delle circostanze del caso concreto.

Il criterio Circumstances of Breach (CB – Circostanze della violazione) valuta elementi complementari a DPC ed EI, ossia la perdita di sicurezza dei dati (confidenzialità, integrità, disponibilità) e l'intenzionalità dolosa. La perdita di confidenzialità si verifica quando informazioni riservate sono accessibili a soggetti non autorizzati; la perdita di integrità quando i dati vengono alterati con potenziali effetti pregiudizievoli; la perdita di disponibilità quando i dati non possono essere consultati, temporaneamente o permanentemente. L'intenzionalità dolosa distingue violazioni accidentali da azioni volontarie finalizzate a danneggiare gli interessati o il titolare del trattamento, aumentando il rischio di uso dannoso dei dati. A differenza di DPC ed EI, i punteggi relativi ai diversi elementi CB si sommano per ottenere

il punteggio finale, poiché più circostanze possono coesistere nella stessa violazione.

Per completare la valutazione della gravità di una violazione di dati personali, la metodologia ENISA prevede una scala di Severity (SE – Gravità) che consente di classificare l'impatto sugli interessati in quattro livelli crescenti. Come evidenziato nel documento ufficiale, allegati al testo principale forniscono tabelle dettagliate per l'assegnazione dei punteggi ai vari criteri e per l'interpretazione della scala.

- Bassa ($SE < 2$): gli interessati non subiscono effetti significativi o incontrano lievi disagi facilmente superabili (es. reinserimento di dati, fastidi minori).
- Media ($2 \leq SE < 3$): gli interessati possono subire inconvenienti rilevanti, comunque gestibili nonostante alcune difficoltà (es. costi aggiuntivi, negato accesso a servizi, stress, piccoli disturbi fisici).
- Alta ($3 \leq SE < 4$): gli interessati affrontano conseguenze significative, superabili con serie difficoltà (es. appropriazione indebita di fondi, blacklist bancarie, danni patrimoniali, perdita del lavoro, peggioramento della salute).
- Molto alta ($SE \geq 4$): gli interessati possono subire conseguenze rilevanti o irreversibili, potenzialmente insormontabili (es. gravi difficoltà economiche, malattie fisiche o psicologiche a lungo termine, morte).

L'impiego di un *Severity Calculator*, anche nella forma di un semplice foglio di calcolo, consente di rendere la misurazione più oggettiva, coerente e specifica. Sebbene il GDPR introduca l'obbligo di notificare le violazioni di dati personali, tale obbligo non sussiste in maniera assoluta e incondizionata.

Ne consegue che, non appena venga a conoscenza di una violazione, il titolare del trattamento non deve soltanto attivarsi per contenerne gli effetti, ma anche procedere a una tempestiva valutazione del rischio derivante

dall'incidente. Tale attività risponde a una duplice finalità: da un lato, consente di adottare misure adeguate di contenimento e mitigazione del danno; dall'altro, permette di stabilire se ricorrano i presupposti per adempiere agli obblighi di notifica verso l'autorità di controllo e, se del caso, di comunicazione agli interessati[354].

3.6 La famiglia degli Standard ISO/IEC 27000

Nel complesso (e sempre in evoluzione) panorama della sicurezza delle informazioni, si riscontra la presenza di una molteplicità di framework normativi e operativi, elaborati con l'intento di fornire alle organizzazioni un insieme coerente di principi, metodologie e strumenti idonei a prevenire e contrastare le condotte che possano compromettere l'integrità, la riservatezza o la disponibilità del patrimonio informativo aziendale. Tali strutture di riferimento assumono pertanto la funzione di quadri concettuali di governance che hanno la capacità di orientare le scelte strategiche in materia di sicurezza digitale e di promuovere una cultura organizzativa fondata sulla consapevolezza del rischio.

In tale prospettiva, i framework si rivelano strumenti di particolare rilievo in quanto offrono un linguaggio comune, condiviso e comprensibile a tutti i livelli dell'organizzazione, favorendo così l'instaurarsi di una visione unitaria e trasversale delle problematiche connesse alla protezione dei dati e alla gestione dei rischi informatici. Essi contribuiscono, pertanto, a ridurre le asimmetrie informative e a promuovere un dialogo efficace fra le diverse funzioni aziendali coinvolte nel governo della sicurezza.

Di conseguenza la scelta del framework di riferimento deve risultare il frutto di un'attenta valutazione del contesto operativo, della struttura

[354] Gruppo di lavoro ex art. 29 sulla protezione dei dati personali (2018), *Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679*, Bruxelles: Commissione europea.

organizzativa e del livello di maturità in materia di sicurezza informatica che caratterizzano l'ente o l'impresa interessata, affinché le misure e le procedure adottate risultino realmente adeguate e proporzionate rispetto ai rischi specifici cui l'organizzazione è esposta.

L'Organizzazione Internazionale per la Standardizzazione (ISO) e la Commissione Elettrotecnica Internazionale (IEC) rappresentano i principali organismi di riferimento per la definizione di standard tecnici a livello globale. L'attività dei suddetti enti mira a garantire che prodotti e servizi rispondano a requisiti uniformi di sicurezza, affidabilità e qualità, in modo da favorire al contempo l'adozione di modelli produttivi fondati su principi di sostenibilità e responsabilità sociale. In tal senso, la standardizzazione assume una valenza non solo tecnica, ma anche giuridico-economica, poiché essa incide anche sulla costruzione di un mercato più equo e competitivo.

Gli enti nazionali membri dell'ISO e dell'IEC partecipano attivamente ai processi di elaborazione normativa attraverso comitati tecnici dedicati ai diversi ambiti di attività. La cooperazione tra tali comitati consente di armonizzare gli interventi e di sviluppare sinergie tra le due organizzazioni, assicurando coerenza e continuità nella produzione degli standard internazionali. Nel contesto dell'information security, i framework sviluppati e adottati a livello internazionale possono essere ricondotti, sia dal punto di vista concettuale che funzionale, a tre macro-categorie. Una prima categoria è rappresentata dai framework di controllo, i quali si configurano come raccolte sistematiche di controlli fondamentali che le organizzazioni sono chiamate a implementare al fine di assicurare un livello minimo ma strutturato di protezione del proprio patrimonio informativo. Tali framework si distinguono per la loro funzione eminentemente prescrittiva e operativa, in quanto mirano a fornire un elenco di misure concrete da applicare, spesso in modo scalabile, in relazione alla complessità e alle dimensioni dell'organizzazione.

Accanto a essi si collocano i framework di requisiti, che si occupano di definire l'insieme dei requisiti essenziali che devono essere soddisfatti per la progettazione, l'implementazione, il mantenimento e il miglioramento continuo di un sistema di gestione della sicurezza delle informazioni. Tali framework, generalmente suscettibili di certificazione, pongono l'accento non tanto sui singoli controlli, quanto piuttosto sulla strutturazione di un modello organizzativo complessivo, ispirato a principi di governance e miglioramento costante.

Infine, una terza categoria è costituita dai framework di rischio, che hanno ad oggetto la descrizione e la regolazione del processo di gestione del rischio informatico, ossia l'insieme delle attività volte all'identificazione, alla valutazione, al trattamento e al monitoraggio continuo dei rischi che incombono sul sistema informativo. I framework descritti si distinguono per la loro natura metodologica, ponendo al centro la valutazione del rischio come strumento decisionale e di indirizzo strategico, in grado di orientare in modo coerente la selezione delle misure di sicurezza e la pianificazione delle politiche di protezione dei dati.

La cosiddetta "famiglia" delle norme ISO/IEC 27000 costituisce un articolato corpus regolamentare di matrice internazionale, volto a disciplinare in modo sistematico l'insieme delle prassi e dei requisiti inerenti alla gestione della sicurezza delle informazioni all'interno delle organizzazioni pubbliche e private. In tale ambito, la norma ISO/IEC 27001 riveste un ruolo centrale, in quanto individua e documenta i requisiti necessari per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI), configurandosi pertanto come lo standard di riferimento per la certificazione di conformità in materia.

Accanto ad essa, la ISO/IEC 27002 si pone quale strumento di indirizzo e di supporto operativo, fornendo linee guida per la selezione, l'implementazione e la gestione dei controlli di sicurezza, con finalità applicative e di contestualizzazione delle misure previste. Tale norma, a

differenza della 27001, non è suscettibile di certificazione, in quanto priva di requisiti vincolanti, ma si limita a offrire un insieme strutturato di raccomandazioni di carattere tecnico e organizzativo.
Tali standard si occupano di descrivere una panoramica e il vocabolario dei sistemi di gestione della sicurezza delle informazioni, facendo riferimento alla famiglia di norme del sistema di gestione della sicurezza delle informazioni (includendo l'ISO/IEC 27003, l'ISO/IEC 27004 e l'ISO/IEC 27005) con i termini e le definizioni ad essi correlati.

Come discusso, ogni organizzazione od azienda si occupa, anche in maniera incidentale, di trattare dati personali, ovvero informazioni riconducibili ad una persona identificata o identificabile. Quantità e varietà dei dati personali elaborati sono in aumento costante, così come il numero di situazioni in cui un'organizzazione si trova nella situazione di dover cooperare con altre organizzazioni riguardo l'elaborazione di questa tipologia di informazioni. La protezione della privacy nel contesto dell'elaborazione dei dati personali è una necessità sociale, nonché oggetto di legislazione e/o regolamentazione dedicata in tutto il mondo. In questo contesto si aggiunge il Sistema di Gestione della Sicurezza delle Informazioni (Information Security Management System[355]) definito nello standard ISO/IEC 27001[356], progettato per consentire l'aggiunta di requisiti specifici per settore, senza la necessità di sviluppare un nuovo Sistema di Gestione. Gli standard per i Sistemi di Gestione ISO, compresi quelli specifici per settore, sono progettati per poter essere implementati separatamente o come un Sistema di Gestione combinato. I requisiti e le linee guida per la protezione dei dati personali variano a seconda del contesto dell'organizzazione, in particolare dove esistono legislazioni e/o regolamenti nazionali. La norma ISO/IEC 27701

[355] "ISMS".
[356] Lo standard è attualmente in fase di revisione e verrà aggiornato nei prossimi mesi: ISO/IEC. (2019). *ISO/IEC 27701:2019 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. ISO/IEC.

introduce un insieme dettagliato di check-list operative, concepite per essere adattabili a differenti contesti normativi internazionali, consentendo alle organizzazioni di armonizzare le proprie pratiche di trattamento dei dati con i principi sanciti, ad esempio, dal Regolamento (UE) 2016/679 (GDPR) o da altre legislazioni di settore.

In tale prospettiva, le imprese che adottano lo standard sono tenute a documentare in modo sistematico le proprie politiche, procedure, protocolli e attività operative, conformemente alle liste di controllo previste dalla norma. Tale documentazione, che costituisce parte integrante del sistema di gestione, è oggetto di verifica periodica da parte di auditor interni e di organismi di terza parte, i quali accertano la conformità effettiva ai requisiti dello standard e rilasciano evidenze formali del rispetto delle prescrizioni in materia di protezione dei dati personali.

L'implementazione della ISO/IEC 27701 comporta una serie di vantaggi sostanziali per le organizzazioni che intendano rafforzare la propria postura in materia di sicurezza e compliance. In particolare, tale certificazione[357]:

- Contribuisce a consolidare la fiducia degli stakeholder nella capacità dell'organizzazione di gestire in modo responsabile le informazioni personali.
- Assicura un più elevato grado di trasparenza nei rapporti tra le diverse parti interessate.
- Facilita la conclusione di accordi commerciali e partnership, grazie alla dimostrata conformità a standard riconosciuti a livello globale.
- Chiarisce ruoli e responsabilità nell'ambito dei processi di trattamento dei dati, riducendo le aree di ambiguità organizzativa.

[357] SQS, *ISO 27701 – Sistema di Gestione per la Protezione dei Dati Personali*, disponibile online: https://www.sqs.it/iso27701.html, consultato il 13 novembre 2025.

- Supporta l’adempimento delle normative nazionali e sovranazionali in materia di privacy.
- Mitiga il rischio di sanzioni e responsabilità derivanti da violazioni delle disposizioni internazionali sulla protezione dei dati.
- In tal modo, la norma ISO/IEC 27701 si configura non soltanto come uno strumento tecnico di gestione della privacy, ma come un vero e proprio modello di governance orientato alla responsabilizzazione organizzativa, in linea con i principi di accountability e di tutela sostanziale dei diritti degli interessati.

CAPITOLO IV
EUROPEAN HEALTH DATA SPACE (EHDS)

Sommario: 4.1 Lo Spazio Europeo dei Dati Sanitari – 4.2 La protezione dei dati sanitari – 4.3 Il riutilizzo dei dati sanitari per uso primario – 4.4 Il riutilizzo dei dati sanitari per uso secondario

4.1 Lo Spazio Europeo dei Dati Sanitari

La tutela della salute incide in modo determinante sull'effettiva libertà personale dell'individuo e sulla possibilità di sviluppare pienamente la propria personalità; tali esigenze impongono alla Repubblica il dovere di rimuovere gli ostacoli che ne limitano la realizzazione, ai sensi dell'art. 3, secondo comma, della Costituzione[358].

Nel contesto in esame, l'evoluzione tecnologica assume un ruolo fondamentale, influenzando le dinamiche del diritto alla salute in molteplici direzioni[359].

Esiste un notevole interesse a livello internazionale nello sfruttamento del potenziale delle soluzioni digitali per migliorare la qualità e la sicurezza dell'assistenza sanitaria. L'implementazione di tecnologie *eHealth trasformative* (quelle soluzioni digitali in grado di modificare in profondità, e non solo migliorare marginalmente, il modo in cui i sistemi sanitari operano) è già in corso in diversi Paesi, spesso con investimenti

[358] È importante sottolineare che, data l'ampiezza potenziale del concetto di salute, non tutte le richieste di prestazioni sanitarie rientrano nel cosiddetto "nucleo irriducibile del diritto alla salute protetto dalla Costituzione come ambito inviolabile della dignità umana" (Corte costituzionale, 509/2000). Al di fuori di questo ambito, l'effettiva esigibilità delle prestazioni sanitarie da parte della Repubblica è soggetta al bilanciamento con altri valori, inclusa la sostenibilità economica delle finanze pubbliche. D'altra parte, il rispetto della persona umana richiede di contenere l'ingerenza pubblica sul soggetto, anche quando sia prevista, per legge, l'imposizione di trattamenti sanitari obbligatori (art. 32, secondo comma, Cost.).

[359] C. SARRA, *Il diritto alla salute nell'era della datificazione*, in a cura di C. SARRA, A. ZILIO, G. DE BONA, *Diritto alla salute, protezione dei dati personali e intelligenza artificiale.* FrancoAngeli, Milano, 2025, 13.

significativi[360]. Un punto di riferimento fondamentale nella definizione del concetto di e-health è offerto da G. Eysenbach, uno dei pionieri in questo ambito, che descrive l'e-health come: *"Un campo emergente che si colloca all'incrocio tra informatica medica, sanità pubblica e ambito economico, e riguarda i servizi e le informazioni sanitarie forniti o potenziati attraverso Internet e le tecnologie correlate. In senso più ampio, il termine non indica solo un progresso tecnico, ma rappresenta anche uno stato d'animo, un modo di pensare, un atteggiamento e un impegno orientati a una visione globale e interconnessa, con l'obiettivo di migliorare l'assistenza sanitaria a livello locale, regionale e mondiale grazie all'uso delle tecnologie dell'informazione e della comunicazione*[361]*."*

I termini *e-health* e *digital health* sono spesso utilizzati in modo intercambiabile, pur potendo assumere significati parzialmente differenti a seconda del contesto. In via generale, con *e-health* si fa riferimento all'impiego di tecnologie elettroniche finalizzate all'erogazione di servizi e informazioni sanitarie, mentre la nozione di *digital health* appare più ampia, comprendendo un ventaglio di applicazioni e strumenti che spaziano dalla *mobile health* alla telemedicina, fino ai dispositivi indossabili. La definizione e la portata di tali concetti, tuttavia, possono variare in relazione alle fonti e agli ambiti in cui vengono utilizzati.

Secondo lo *European Programme of Work 2020–2025* dell'Organizzazione Mondiale della Sanità[362], la *digital health* estende il concetto di *e-health* a ulteriori settori, quali:

---

[360] A.D. BLACK et al., *The Impact of eHealth on the Quality and Safety of Health Care: A Systematic Overview*, in *PLoS Medicine*, 2011, 8(1), 1-3.
[361] G. EYSENBACH, *What is e-health?*, in *Journal of Medical Internet Research*, 2001, 3(2), 1-2.
[362] *WHO European Programme of Work 2020-2025 (EPW) – "United action for better health in Europe"*, World Health Organization, Regional Office for Europe, https://www.who.int/europe/news/item/13-09-2022-countries-in-the-european-region-adopt-first-ever-digital-health-action-plan, consultato da ultimo l'8.10.2025.

- La telemedicina, volta a garantire l'accesso ai servizi sanitari indipendentemente dal luogo di residenza.
- I dati sanitari e i sistemi informativi sanitari, strumenti indispensabili per consentire alle autorità di elaborare politiche di salute pubblica.
- L'intelligenza artificiale e i *big data*, che supportano medici, operatori e policy makers nella programmazione e attuazione di interventi.
- Il contrasto all'"infodemia" online[363], favorendo la diffusione di informazioni sanitarie affidabili e di qualità[364].

L'Unione europea rappresenta un modello peculiare di integrazione in ambiti che, tradizionalmente, rientrano nella sfera di competenza esclusiva dei singoli Stati. Attualmente l'UE comprende circa 450 milioni di cittadini distribuiti in 27 Stati nazionali, caratterizzati dall'uso di 24 lingue ufficiali, tutte riconosciute come parimenti valide. Il diritto dell'Unione gode di primazia rispetto agli ordinamenti interni, e il processo di integrazione tende progressivamente ad approfondirsi. Tuttavia, ciascuno Stato membro porta con sé un retaggio di decenni, se non secoli, di evoluzione autonoma, che si traduce in consuetudini e visioni giuridiche differenti. L'evoluzione normativa e procedurale nei vari paesi si è svolta in maniera indipendente e, con ogni probabilità, tali diversità permarranno anche in futuro. Lo stesso fenomeno si osserva nel settore della sanità digitale: i sistemi di *eHealth* sono stati introdotti nei diversi Paesi molto tempo prima dell'avvio delle attuali iniziative di armonizzazione, determinando un quadro frammentato che oggi rende particolarmente complesso il processo di unificazione[365].

---

[363] Su questo tema si veda: C. LOBASCIO, *Droit et désinformation sanitaire: réponses juridiques et défis en Europe et en Italie*, in *Journal de droit de la santé et de l'assurance maladie*, 2025, 43.
[364] R. ORĂȘTEAN, R. SAVA, S. MĂRGINEAN, *Measuring healthcare digitalisation in the European Union: Trends and challenges*, in *Revista Economică*, 2022, 74(4), 64-74.
[365] J. BRUTHANS, *Connecting the Electronic Medical Records in the European Union – Where Do We Stand and Where Does It Go?*, in *Telehealth and Medicine Today*, 2024, 9(2), 1.2.

Nel contesto di riferimento il concetto di *data governance* assume significati differenti a seconda degli stakeholder coinvolti, circostanza prevedibile in un'epoca in cui le possibilità di raccolta, utilizzo e analisi dei dati crescono in modo esponenziale, sia in termini quantitativi che di rapidità di elaborazione. Per gli stakeholder che sostengono i diritti dei pazienti, la *data governance* si identifica prevalentemente con il rigoroso controllo individuale sui propri dati personali e sulla loro eventuale trasmissione o ulteriore utilizzazione: una concezione dunque essenzialmente protettiva. All'estremo opposto, vi è chi interpreta la *data governance* come lo strumento per assicurare l'impiego ottimale di una risorsa preziosa, pur nel rispetto delle garanzie dovute alle fonti dei dati.

Tra queste due visioni si collocano posizioni intermedie, che pongono l'accento in misura variabile ora sulla protezione, ora sulla valorizzazione del dato, spesso soffermandosi su aspetti di natura più tecnica: ad esempio, garantire l'elevata qualità delle informazioni, la conformità a standard condivisi o la loro conservazione in ambienti sicuri. In tale prospettiva, la *data governance* può essere intesa come l'insieme dei processi volti a regolare la disponibilità, l'usabilità, l'integrità e la sicurezza dei dati all'interno dei sistemi informativi, sulla base di standard e politiche interne che ne disciplinano l'uso. Una *data governance* efficace, in questo senso, consente di assicurare che i dati siano affidabili, coerenti e non soggetti ad abusi[366].

Nel corso del Discorso sullo Stato dell'Unione del 2020, la Presidente della Commissione Europea Ursula von der Leyen ha annunciato la nuova proposta legislativa volta alla creazione dell'European Health Data Space (EHDS). L'obiettivo dichiarato di tale iniziativa consiste nel rendere accessibili i dati sanitari elettronici, al fine di sostenere l'erogazione dei

[366] HORGAN, D., et al., *European Health Data Space – An Opportunity Now to Grasp the Future of Data-Driven Healthcare*, in *Healthcare (Basel)*, 2022, 10, 2-5.

servizi sanitari, promuovere la ricerca e l'innovazione nel settore, migliorare l'elaborazione di politiche pubbliche e la regolamentazione, nonché favorire lo sviluppo di modelli di medicina personalizzata. Nel maggio 2022, la Commissione Europea ha presentato una proposta legislativa per l'istituzione dell'European Health Data Space (EHDS). Il regolamento si configura come un quadro normativo integrato, comprendente regole, standard e prassi comuni, infrastrutture digitali e un modello di governance, destinato a disciplinare l'uso dei dati sanitari elettronici sia a livello nazionale sia transfrontaliero nell'Unione Europea.

Il 21 gennaio 2025, il Consiglio dell'Unione Europea ha annunciato l'adozione della normativa che istituisce lo Spazio Europeo dei Dati Sanitari (Regolamento UE 2025/327) conformemente alla proposta formulata nel 2022. Tale regolamento modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847, segnando il primo intervento normativo settoriale derivante dalla Strategia Europea per i Dati del 2020[367].

Quest'ultima delinea la costituzione di un mercato unico dei dati fondato su regole e valori comuni, e rappresenta la traduzione operativa di principi quali la protezione dei diritti fondamentali dei pazienti, la promozione della libera circolazione dei dati e l'integrazione digitale dei sistemi sanitari. Da un punto di vista dottrinale, l'EHDS può essere interpretato come un tentativo di conciliare il principio di sussidiarietà, che riserva agli Stati membri la competenza primaria in materia sanitaria, con la necessità di creare un ecosistema europeo dei dati sanitari interoperabile e sicuro, capace di sostenere politiche pubbliche basate sui dati e innovazioni tecnologiche[368].

[367] S. THOBANI, *Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space)*, in *Persona e Mercato*, 2024, 4, 1393-1399.
[368] D. FÅHRÆUS, J. REICHEL, S. SLOKENBERGA, *The European Health Data Space: Challenges and Opportunities*, Stockholm, Sieps, 2024, 19-20.

L'Unione Europea infatti ha esercitato un ruolo storico nel settore della sanità pubblica[369], pur trovandosi vincolata dal principio di sussidiarietà sancito dall'art. 5 TUE, che attribuisce agli Stati membri la competenza primaria in materia di tutela della salute. In questo contesto, l'istituzione dell'European Health Data Space (EHDS) rappresenta un tentativo di armonizzare il quadro europeo dei dati sanitari, rispondendo a esigenze emerse sia in termini di salute pubblica sia di tutela dei diritti fondamentali dei pazienti.

L'EHDS riflette la convergenza di diversi sviluppi recenti della politica sanitaria e della regolamentazione dei dati. Innanzitutto, la pandemia di COVID-19 ha evidenziato la necessità di rafforzare le capacità dell'UE nella promozione della salute pubblica, richiamando l'attenzione sulla gestione transfrontaliera dei dati sanitari e sull'importanza di strumenti coordinati a livello sovranazionale. In secondo luogo, è stata riconosciuta la limitata effettività dei diritti dei pazienti previsti dal GDPR, la cui applicazione nel settore sanitario incontra ostacoli operativi e frammentazioni normative. In terzo luogo, la Commissione europea ha promosso una politica volta a rendere i dati sanitari e non sanitari accessibili per finalità di ricerca, sia commerciale sia non commerciale, integrando la logica della libera circolazione dei dati (art. 16 TFUE) con quella della protezione dei diritti fondamentali. Infine, la dottrina e la prassi hanno evidenziato l'inefficacia dei

[369] Si ricorda la Carta dei diritti fondamentali dell'Unione europea, la quale pone al centro la tutela della dignità umana (art. 1), il diritto alla vita (art. 2), l'inviolabilità dell'integrità della persona (art. 3), il divieto di tortura e di trattamenti inumani o degradanti (art. 4), il rispetto della vita privata e familiare (art. 7), la protezione dei dati personali (art. 8) e il divieto di discriminazioni, comprese quelle fondate su caratteristiche genetiche (art. 21). Particolare rilievo assume l'art. 3, che sancisce il diritto di ogni individuo al rispetto della propria integrità fisica e psichica. La disposizione, al paragrafo 2, specifica alcuni principi irrinunciabili nel campo della medicina e della biologia: la necessità del consenso libero e informato della persona interessata; il divieto di pratiche eugenetiche, soprattutto se dirette alla selezione degli individui; il divieto di trarre profitto commerciale dal corpo umano e dalle sue parti; il divieto di clonazione riproduttiva degli esseri umani. M. CHAWKI, *Security and privacy in the era of electronic health records (EHRs)*, in *RAIS Journal for Social Sciences*, 2021, 5, 1.

precedenti programmi volontari nel garantire l'accesso e la condivisione dei dati sanitari da parte dei pazienti e nel ridurre la frammentazione e la scarsa interoperabilità dei sistemi digitali sanitari, sia a livello nazionale sia transfrontaliero.

L'EHDS si configura, dunque, come uno strumento normativo e infrastrutturale in grado di coniugare il rispetto dei diritti fondamentali dei pazienti, la promozione della ricerca e dell'innovazione e la costruzione di un ecosistema digitale sanitario europeo più coerente ed integrato. La sua attuazione solleva questioni complesse di bilanciamento tra competenze nazionali e azione europea, interoperabilità tecnica e governance dei dati, che costituiscono oggi oggetto di crescente dibattito dottrinale e giurisprudenziale.

Il regolamento si propone di definire un quadro normativo completo, comprendente regole, standard e prassi comuni, infrastrutture e un modello di governance, destinato sia all'uso primario dei dati sanitari – ossia l'impiego di dati elettronici personali per l'erogazione di servizi sanitari a favore dell'individuo – sia all'uso secondario, cioè l'utilizzo dei dati sanitari elettronici per finalità più ampie, quali la ricerca sanitaria, la definizione di politiche pubbliche o altre attività di interesse collettivo.

A tal fine, l'EHDS si articola su quattro linee di intervento principali:

- Rafforzamento del controllo dei pazienti sui propri dati, garantendo una maggiore effettività dei diritti individuali alla gestione, accesso e condivisione dei dati sanitari, nel rispetto del GDPR;
- Definizione di regole per i sistemi di cartelle cliniche elettroniche (EHR[370]), finalizzate a promuovere affidabilità, sicurezza e

[370] La cartella clinica elettronica trova un espresso riconoscimento a livello sovranazionale nella Raccomandazione della Commissione del 2 luglio 2008 e in quella del 6 febbraio 2019/24, mentre nell'ordinamento interno è disciplinata dall'art. 47-bis del d.l. 9 febbraio 2012, n. 5. Nella Raccomandazione del 2008 essa viene definita come la "*documentazione medica completa, relativa allo stato di salute fisico e mentale, passato e presente, di un individuo, in forma elettronica, che consenta la pronta disponibilità dei dati per finalità di cura e per scopi strettamente connessi*." L'istituzione di una rete transnazionale di cartelle

interoperabilità, così da assicurare un'informazione sanitaria coerente e fruibile a livello nazionale e transfrontaliero;

- Istituzione di regole per l'uso secondario dei dati sanitari, disciplinando modalità, limiti e garanzie per la ricerca, la pianificazione sanitaria e altre applicazioni di interesse pubblico o commerciale;
- Creazione di infrastrutture transfrontaliere obbligatorie, una dedicata all'uso primario e l'altra all'uso secondario, al fine di assicurare una gestione coordinata e standardizzata dei dati sanitari a livello europeo[371].

La prontezza degli Stati membri rispetto all'implementazione dell'European Health Data Space dipende in larga misura da fattori quali

cliniche elettroniche è stata prospettata quale strumento idoneo a garantire l'accessibilità sicura, interoperabile e transfrontaliera dei dati sanitari, perseguendo un duplice obiettivo: da un lato, innalzare la qualità dell'assistenza e contenere i costi del sistema; dall'altro, uniformare i processi di trattamento dei dati sanitari nei diversi ordinamenti nazionali, assicurando la massima tutela della riservatezza.
Su un piano differente si colloca il fascicolo sanitario elettronico, introdotto dall'art. 12, d.lgs. 18 ottobre 2012, n. 179, quale strumento idoneo a raccogliere in formato digitale l'intera storia clinica dell'interessato, includendo dati e documenti sanitari e sociosanitari. La disciplina del FSE è stata poi precisata con il D.P.C.M. 29 settembre 2015, n. 178, che ne ha regolamentato l'attuazione a seguito di una fase di sperimentazione regionale. Rispetto alla cartella clinica elettronica, limitata a un singolo episodio di ricovero, il FSE ha carattere "longitudinale" e richiede un costante aggiornamento dei dati provenienti sia dal paziente che dai professionisti sanitari che lo assistono. L'evoluzione normativa ha ulteriormente ampliato il perimetro del FSE, come avvenuto con il d.l. 19 maggio 2020, n. 34 (*c.d. decreto rilancio*), che ne ha esteso l'ambito anche ai documenti digitali sanitari e sociosanitari prodotti al di fuori del SSN.
Un ulteriore modello è rappresentato dal dossier sanitario elettronico, oggetto delle linee guida del Garante per la protezione dei dati personali del 2015. Esso consiste nell'insieme dei dati generati da eventi clinici passati e presenti relativi al paziente, condivisi tra i professionisti che operano nella medesima struttura sanitaria. Diversamente dal FSE, il dossier è caratterizzato da una *monotitolarità* del trattamento dei dati (in capo alla singola struttura sanitaria) e, a differenza della cartella clinica, non si riferisce a un singolo episodio di ricovero, bensì ricostruisce l'intera storia clinica del paziente all'interno di una determinata struttura. F. CIMBALI, *La governance della sanità digitale*, 3, Wolters Kluwer Italia, 2023, 119-125.

[371] J. S. MARCUS et al., *The European Health Data Space*, in *IPOL - Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament Policy Department Studies*, 2022.

l'esistenza di infrastrutture per la gestione dei dati sanitari, le politiche e le normative vigenti in materia di condivisione dei dati e le capacità tecniche disponibili. Gli Stati membri che hanno già implementato sistemi di cartelle cliniche elettroniche e definito politiche o quadri normativi per la condivisione dei dati sanitari risultano maggiormente preparati a partecipare all'EHDS. Al contrario, gli Stati privi di infrastrutture adeguate o di capacità tecniche e normative necessitano di supporto e investimenti per poter aderire pienamente a tale iniziativa.

Per ridurre efficacemente tali disparità, la Commissione Europea ha destinato specifici finanziamenti a sostegno della preparazione degli Stati membri all'EHDS. In particolare, il programma Horizon 2020 ha finanziato progetti di ricerca e innovazione finalizzati a facilitare la condivisione dei dati sanitari, sviluppando al contempo infrastrutture e formati standardizzati. Inoltre, la Commissione ha istituito un quadro di governance dell'EHDS, volto a garantire la partecipazione di tutti gli Stati membri indipendentemente dal loro livello di preparazione. Tale quadro fornisce indicazioni e supporto agli Stati membri su aspetti quali la protezione dei dati, la sicurezza informatica, l'interoperabilità. oltre a considerazioni etiche, contribuendo a creare un ecosistema digitale sanitario europeo armonizzato e sicuro[372]. Merita rilievo la sensibilità mostrata dal legislatore europeo rispetto alle peculiarità proprie del settore sanitario. È significativo, infatti, che sia stato riconosciuto come i dati sanitari richiedessero un regime differenziato e non potessero essere assimilati, senza distinzioni, ad altre tipologie di informazioni detenute dalle amministrazioni pubbliche. Tale consapevolezza ha rappresentato il presupposto per l'elaborazione di politiche specificamente orientate alla gestione e all'impiego dei dati sanitari[373].

---

[372] S. KYMPOUROPOULOS, *Real World Evidence: methodological issues and opportunities from the European Health Data Space*, in *BMC Medical Research Methodology*, 2023, 23, 185.

[373] G. CARULLO, *Dati sanitari, sistemi sanitari nazionali e riuso dei dati*, in *Sanità rurale e assistenza sanitaria decentrata: Spagna e Italia. Esperienze a confronto = Sanidad rural y*

Il percorso di attuazione dello European Health Data Space si articola in diverse tappe, pensate per permettere agli Stati membri di adeguarsi progressivamente al nuovo quadro europeo sui dati sanitari. La prima scadenza è stata a marzo del 2025, quando il Regolamento EHDS è entrato in vigore, dando il via al periodo transitorio necessario per adattare sistemi normativi e infrastrutture. Due anni dopo, nel marzo 2027, la Commissione europea dovrà adottare gli atti di esecuzione principali, che forniranno indicazioni operative su come applicare concretamente il Regolamento. Nel marzo 2029 diventeranno operative alcune disposizioni chiave. Gli Stati membri dovranno garantire lo scambio delle prime categorie prioritarie di dati sanitari, come i *Patient Summaries* e le prescrizioni elettroniche, mentre le regole sull'uso secondario riguarderanno la maggior parte delle informazioni contenute nelle cartelle cliniche elettroniche. A marzo 2031 sarà la volta della seconda serie di dati prioritari: immagini diagnostiche, referti di laboratorio e lettere di dimissione ospedaliera. Le norme sull'uso secondario si estenderanno alle categorie residue, come i dati genomici, con implicazioni importanti per la protezione dei dati personali e per la ricerca scientifica. Infine, nel marzo 2034, anche Stati terzi e organizzazioni internazionali potranno chiedere di aderire all'infrastruttura *HealthData@EU* per l'uso secondario dei dati, aprendo possibilità di cooperazione internazionale[374].

4.2 La protezione dei dati sanitari

Sebbene nessun ambito della società, sia a livello nazionale che internazionale, risulti escluso dalla rivoluzione digitale, vi sono settori, specie quello sanitario e della salute, particolarmente delicati, che richiedono da un

asistencia sanitaria descentralizada: España e Italia. Experiencia a debat, a cura di C. BOTTARI, P. J. TÁRRAGA LÓPEZ, J. CANTERO MARTÍNEZ, Napoli, Editoriale Scientifica, 2024, 401-420.

[374] European Commission, *Regolamento sull'European Health Data Space (EHDS)*, https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en, consultato da ultimo il 5.3.2025.

lato una riflessione interdisciplinare approfondita e dall'altro un intervento legislativo mirato ed efficace. Ciò si giustifica con il forte impatto potenziale che le innovazioni digitali possono avere su ciascun individuo, considerando le condizioni di vulnerabilità temporanea o permanente derivanti dall'insorgenza di diverse patologie, le quali non solo colpiscono direttamente la persona interessata, ma influenzano anche la sua rete familiare e sociale[375].

L'informazione in ambito medico rappresenta un elemento essenziale per la definizione della cura appropriata. Spetta al medico raccogliere, organizzare e interpretare i dati del paziente, al fine di formulare una diagnosi quanto più accurata possibile. La medicina può dunque essere intesa come un flusso informativo proveniente dal paziente e relativo al paziente, che trova oggettivazione attraverso l'aggregazione informatizzata dei dati di ciascun individuo sottoposto a trattamento sanitario.

Un'informazione medica si trasforma in dato sanitario nel momento in cui viene sottoposta a manipolazione da parte dell'operatore, diventando così elemento documentale, anche in formato elettronico. Tale trasformazione impone all'operatore sanitario un obbligo di tutela di diritti, tra cui quello alla riservatezza e alla protezione dei dati personali. Si può affermare che i dati sanitari assumono non solo un valore scientifico, ma anche economico, generando rischi specifici che rendono necessaria una protezione adeguata del paziente[376].

L'impiego delle tecnologie in ambito sanitario costituisce un elemento fondamentale per la tutela della salute pubblica e la sicurezza collettiva, nonché per l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie, andando a contribuire al miglioramento

[375] G. FIORIGLIO, *La protezione dei dati sanitari nella società algoritmica. Profili informatico-giuridici*, in *Journal of Ethics and Legal Technologies*, 2021, 3(2), 79-102.
[376] G. PREITE, *L'habeas data sanitario come diritto all'autodeterminazione digitale del paziente*, in *Rivista elettronica di diritto, economia, management*, 2014, 105-116.

complessivo dei sistemi sanitari. Tuttavia, la rilevanza degli interessi giuridici coinvolti impone un rafforzamento delle garanzie di tutela, in particolare con riguardo alla protezione dei dati personali[377]. In tale contesto, la disciplina europea sull'intelligenza artificiale ha incluso la protezione della salute tra i propri obiettivi prioritari, riconoscendo la necessità di delineare limiti allo sfruttamento economico dei dati sanitari, in coerenza con il principio di precauzione e con l'obiettivo di garantire un equilibrio tra innovazione tecnologica e tutela dei diritti fondamentali degli individui[378].

I dati relativi alla salute costituiscono una categoria speciale di dati, riconosciuta già dalla Convenzione n. 108/1981 (c.d. Convenzione di Strasburgo), primo strumento internazionale volto a garantire la protezione delle persone rispetto al trattamento automatizzato dei dati personali. La stessa Convenzione, insieme alla Raccomandazione n. 81 del Comitato dei Ministri del Consiglio d'Europa, sanciva il principio cardine secondo cui, senza il consenso espresso e consapevole dell'interessato, l'esistenza e il contenuto di un dossier sanitario non potevano essere comunicati a soggetti esterni alle cure mediche, alla sanità pubblica o alla ricerca, se non nei limiti consentiti dal segreto professionale. Questo perché, storicamente, così come nell'attuale prospettiva dei diritti umani, le informazioni sanitarie dei pazienti sono state tutelate dal principio della riservatezza medica. Tale principio trova fondamento nel peculiare rapporto di fiducia che si instaura tra il paziente e il professionista sanitario, rapporto che possiede anche una rilevante dimensione etica. La riservatezza consente al medico di condividere dati personali con terzi soltanto in via eccezionale e in presenza di ragioni giustificative, quali, ad esempio, la tutela dell'interesse pubblico o la

[377] G. SDANGANELLI, *Il diritto all'oblio oncologico e i limiti all'uso dei dati sanitari nell'assicurazione digitale*, in *Federalismi.it*, 2025, 12, 230-252.

[378] L'art. 59, comma 1, lettera a), del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, stabilisce regole armonizzate in materia di intelligenza artificiale e modifica diversi atti normativi preesistenti, tra cui i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139, (UE) 2019/2144, nonché le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

salvaguardia della salute del paziente. L'obbligo di confidenzialità posto a carico dell'operatore sanitario garantisce, pertanto, che l'impiego delle informazioni raccolte resti circoscritto ai soli fini strettamente necessari[379].

In Italia, la legge n. 675/1996 aveva già disciplinato in maniera più rigorosa i dati sanitari, annoverandoli tra i c.d. dati sensibili (artt. 22-23)[380], prevedendo il consenso specifico dell'interessato e forme di tutela rafforzata. Con il successivo Codice della privacy (d.lgs. n. 196/2003) la centralità del consenso è stata ribadita come condizione di liceità del trattamento dei dati personali, in particolare per finalità di cura. Nel sistema allora vigente, il trattamento dei dati sanitari avveniva secondo il cosiddetto "doppio binario": l'art. 26 prevedeva il principio del consenso scritto dell'interessato e della previa autorizzazione del Garante, ma consentiva anche trattamenti senza consenso in casi particolari, come la salvaguardia della vita o dell'incolumità di terzi, sempre subordinati all'autorizzazione del Garante (art. 26, comma 4).

Con l'entrata in vigore del GDPR e del d.lgs. 101/2018 di recepimento, sono intervenute rilevanti novità: i dati relativi alla salute comprendono oggi anche i dati genetici e biometrici (art. 4 GDPR) e non rientrano più nella nozione tradizionale di 'dato sensibile', ma costituiscono una categoria particolare di dati personali (art. 9 GDPR), con misure di protezione rafforzate e specificamente calibrate sulle esigenze di tutela dei

---

[379] S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI, *The European Health Data Space: Examining a New Era in Data Protection*, 1ª ed., Routledge, 2025.

[380] L'art. 22 della legge n. 675/1996, recante la disciplina dei c.d. "dati sensibili", annoverava tra questi anche i dati sanitari, definendoli come "dati personali idonei a rivelare lo stato di salute". Tale formulazione aveva dato luogo a non poche incertezze interpretative, poiché non era sempre agevole stabilire quando un'informazione potesse effettivamente considerarsi idonea a rivelare le condizioni sanitarie di un individuo. Se, da un lato, era indubbio che la menzione di una patologia in atto consentisse di desumere lo stato di salute del soggetto, dall'altro, appariva problematico ricondurre a tale nozione le informazioni relative a malattie ormai superate, prive di effetti sul presente e senza potenziali conseguenze sul futuro dell'interessato. La locuzione "stato di salute" veniva, pertanto, generalmente riferita ad una condizione attuale, eventualmente comprensiva di pregresse patologie solo nella misura in cui queste risultassero idonee ad incidere sul quadro clinico futuro del soggetto, con esclusione, invece, di quelle definitivamente risolte. F. DI CIOMMO, *Trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e Responsabilità*, 2002, 2, 121-134.

diritti fondamentali degli interessati[381]. Ai sensi dell'art. 4, par. 15, GDPR, per 'dati relativi alla salute' si intendono i dati personali attinenti alla salute fisica o mentale di una persona fisica, inclusa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni sul suo stato di salute[382]. Più nel dettaglio, I dati genetici attengono alle caratteristiche ereditarie o acquisite di una persona fisica, desumibili dall'analisi di un campione biologico, idoneo a fornire informazioni univoche sulla fisiologia o sullo stato di salute dell'individuo. I dati biometrici, invece, si riferiscono a caratteristiche fisiche, fisiologiche o comportamentali della persona, ottenute attraverso uno specifico trattamento tecnico[383].

Al fine di fornire una visione sintetica – seppur non esaustiva – delle principali categorie di dati trattati nello Spazio Europeo dei Dati Sanitari (EHDS) e, più in generale, nell'ecosistema digitale della salute, la seguente tabella distingue le tipologie di dati, alcuni esempi rappresentativi e i principali soggetti che li detengono o trattano[384].

Tabella 6 Tipologie di dati relativi alla salute.

Tipologia di dato	**Esempi**	**Titolari o responsabili del trattamento**
Dati clinici	Dati anagrafici del paziente, anamnesi, vaccinazioni, referti	Medici, ospedali, strutture sanitarie

[381] G. SARTORIS, *La tutela dei dati personali dei pazienti di fronte alle sfide della sanità digitale*, in *Diritto e Salute*, 2023, 33-46.
[382] C. SARRA, *Il diritto alla salute nell'era della datificazione*, in *Diritto alla salute, protezione dei dati personali e intelligenza artificiale*, a cura di C. SARRA, A. ZILIO, G. DE BONA, FrancoAngeli, Milano, 2025, 31-33.
[383] B. BUZZELLI, *Dati sanitari e implementazione dell'Intelligenza Artificiale. Health data and implementation of Artificial Intelligence*, in *Intelligenza Artificiale e Sanità Digitale*, a cura di R. PICCOLO, Il Sileno Edizioni, 2024, 45-59.
[384] I. LIANOS, *Access to Health Data, Competition, and Regulatory Alternatives: Three Dimensions of Fairness*, in *Journal of Competition Law & Economics*, 2025, 44-46.

	diagnostici, cartelle cliniche, parametri vitali	
Dati da trial clinici	Dati di sperimentazioni cliniche, risultati di ricerca e sviluppo in fase precoce	Aziende farmaceutiche, centri di ricerca, ospedali universitari
Dati sullo stile di vita	Abitudini alimentari, attività fisica, qualità del sonno, dati su emozioni e abitudini	Motori di ricerca, app di monitoraggio, smartwatch, smartphone, marketplace digitali
Dati da dispositivi sanitari	Dati raccolti da sensori intelligenti, dispositivi indossabili (wearable devices), applicazioni di telemedicina	Produttori di dispositivi medici, aziende ICT, sviluppatori di app
Dati medici e storici	Informazioni su interventi chirurgici, terapie, farmaci assunti, risultati di esami	Professionisti sanitari, ospedali, assicurazioni sanitarie, archivi sanitari elettronici
Dati genetici e '*omics*'	DNA (genomica), RNA (trascrittomica), proteomica, metabolomica	Aziende di test genetici (es. *AncestryDNA*), servizi di *biobanking*, laboratori di ricerca
Dati finanziari e relativi all'assunzione di farmaci	Prescrizioni farmaceutiche, spesa sanitaria, dati su ospedalizzazioni e mortalità	Autorità sanitarie pubbliche, compagnie assicurative, centri statistici nazionali

Dati finanziari sanitari	Pagamenti a medici, spese per ricoveri, transazioni per servizi sanitari	Istituti finanziari, banche, società di carte di credito

L'art. 9, par. 1, GDPR stabilisce il divieto di trattamento dei dati genetici e biometrici intesi a identificare in modo univoco una persona, dei dati relativi alla salute e di quelli riguardanti la vita sessuale o l'orientamento sessuale dell'individuo. Tale divieto, tuttavia, non è assoluto: l'art. 9, par. 2, GDPR prevede numerose eccezioni, tra le quali si segnalano le seguenti più rilevanti:

- Il consenso esplicito dell'interessato;
- Il rispetto della normativa in materia di diritto del lavoro, sicurezza sociale e protezione sociale;
- La tutela dell'interesse vitale dell'interessato o di un'altra persona fisica;
- I dati resi manifestamente pubblici dall'interessato;
- L'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o l'esercizio di funzioni giurisdizionali;
- Motivi di interesse pubblico, purché proporzionati rispetto alla finalità perseguita;
- Finalità di medicina preventiva o del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, gestione di sistemi e servizi sanitari o sociali, sulla base del diritto dell'Unione o nazionale o di un contratto con un professionista della salute;
- Motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di elevati standard di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici.

Tale disciplina evidenzia come il GDPR contempli un equilibrio tra tutela dei dati personali sensibili e esigenze di interesse pubblico, consentendo il trattamento dei dati sanitari solo in presenza di condizioni rigorosamente definite e proporzionate.

Le considerazioni sull'importanza del consenso in ambito sanitario[385] conducono a riflettere sulle problematiche connesse all'art. 22 GDPR, che ha suscitato particolare attenzione in dottrina. L'articolo disciplina le decisioni automatizzate che producono effetti giuridici sull'interessato, prevedendo, tra le eccezioni, il caso in cui la decisione si fondi sul consenso esplicito dell'interessato (par. 2, lett. a). In tale evenienza, il titolare del trattamento deve adottare misure idonee a tutelare i diritti, le libertà e i legittimi interessi dell'interessato, garantendo almeno il diritto a un intervento umano, a esprimere un'opinione e a contestare la decisione (par. 3). Ciò che distingue queste disposizioni rispetto ad altre norme sulla protezione dei dati non è tanto la sicurezza del trattamento automatizzato in sé, quanto l'attenzione posta sulle decisioni che incidono giuridicamente sull'individuo, collocando la disciplina in una prospettiva di protezione più avanzata e mirata ai diritti fondamentali[386].

In questo contesto i sistemi di controllo basati su algoritmi sollevano numerose questioni in materia di diritti fondamentali, dalla protezione della privacy alla tutela dei dati personali, fino alla compressione di libertà essenziali, come quella di movimento. In una prospettiva complessiva, i

[385] Il consenso informato concerne direttamente il trattamento sanitario e il tipo di cure erogate, mentre il consenso privacy si riferisce all'autorizzazione al trattamento dei dati personali per le finalità indicate nell'informativa. I dati relativi alla salute, inclusi i dati genetici e biometrici, possono essere trattati lecitamente per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria, nonché per scopi sociali quali la gestione dei servizi socio-sanitari e per motivi di interesse pubblico nel settore della sanità pubblica. Per tutte le altre finalità, invece, è necessaria l'esplicita manifestazione di consenso libero e specifico da parte dell'interessato. A. PIETROLETTI, A. NICOTRA, *Tutela della salute, sistemi digitali e privacy*, in *Rivista Italiana di Informatica e Diritto*, 2022, 4, 1, 283-294.

[386] P. LOMBARDI, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, in *Il Diritto dell'Economia*, 2021, 67, 106 (3), 49-82.

benefici immediati derivanti dall'adozione di tali tecnologie devono essere confrontati con gli effetti che potrebbero consolidarsi nel lungo periodo.

Come osserva il filosofo Y. N. Harari in un'articolata riflessione sul *Financial Times*, i rischi associati alla sorveglianza di massa si sono evoluti con le emergenze sanitarie: se in passato l'interesse governativo si concentrava sulle attività digitali dell'individuo, in seguito, in contesti come la pandemia da coronavirus, l'attenzione si è spostata su parametri fisici e biometrici, quali temperatura corporea e pressione sanguigna, evidenziando come la tecnologia possa estendere il controllo sulle dimensioni più intime della vita personale[387]: "*Surveillance must always go both ways. If surveillance goes only from top to bottom, this is the high road to dictatorship. So whenever you increase surveillance of individuals, you should simultaneously increase surveillance of the government and big corporations too.* […] *Never allow too much data to be concentrated in only one place. Not during the epidemic, and not when it is over. A data monopoly is a recipe for dictatorship. So if we collect biometric data on people to stop the pandemic, this should be done by an independent health authority rather than by the police*"[388]. Piuttosto che proporre una contrapposizione netta o richiedere una scelta tra la tutela della salute e quella della privacy, è necessario intraprendere un costante bilanciamento tra valori e diritti, entrambi fondamentali. In tale prospettiva vanno interpretate alcune delle principali problematiche emerse e affrontate durante il periodo pandemico, che hanno posto in luce la complessità delle scelte regolatorie e dei trade-off tra sicurezza sanitaria e protezione dei dati personali[389]. È doveroso ricordare

[387] G. DELLA MORTE, *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/, consultato da ultimo il 7.11.2025.
[388] Y. N. HARARI, *Lessons from a year of Covid*, *Financial Times*, 8 luglio 2020, https://www.ft.com/content/f1b30f2c-84aa-4595-84f2-7816796d6841, consultato da ultimo il 7.11.2025.
[389] A. PIETROLETTI, A. NICOTRA, *Tutela della salute, sistemi digitali e privacy*, in *Rivista Italiana di Informatica e Diritto*, 2022, 4, 1, 283-294.

inoltre che la sicurezza dei sistemi informativi sanitari e la protezione dei dati personali vanno analizzati come due aspetti distinti ma strettamente complementari, entrambi finalizzati alla tutela dei sistemi informatici e delle persone. Le tecnologie dedicate alla sicurezza, infatti, mettono a disposizione strumenti idonei a proteggere le informazioni relative agli individui, garantendo al contempo un livello di fiducia tale da consentire agli interessati, quando necessario, di esprimere liberamente il proprio consenso. In questo senso, "security" e "privacy" non si escludono a vicenda, ma operano congiuntamente per assicurare la salvaguardia dei dati e dei diritti degli utenti[390].

4.3 Il riutilizzo dei dati sanitari per uso primario

Il Regolamento sullo Spazio Europeo dei Dati Sanitari introduce un quadro organico finalizzato a garantire la condivisione e la valorizzazione dei dati sanitari in ambito europeo. L'intervento normativo stabilisce principi comuni, regole tecniche e un'infrastruttura di riferimento per la gestione coordinata dei dati, configurando un sistema di governance volto a favorire un accesso ordinato e sicuro alle informazioni sanitarie elettroniche.

Tale impianto si colloca in un rapporto di complementarità rispetto al GDPR e all'AI Act, con i quali condivide finalità e strumenti, ma rispetto ai quali introduce specificazioni settoriali, soprattutto in relazione alla gestione del rischio e alla tutela dei diritti fondamentali degli interessati.

Uno degli elementi di maggiore innovazione è rappresentato dalla creazione di una rete transnazionale che consente l'interoperabilità dei sistemi informativi sanitari nazionali e disciplina in modo distinto l'uso primario dei dati, connesso all'assistenza sanitaria, e l'uso secondario, destinato alla

[390] M. FARINA, *Il cloud computing in ambito sanitario tra security e privacy*, Giuffrè Francis Lefebvre, 2019, 1-3.

ricerca scientifica, alla formulazione di politiche pubbliche e all'innovazione tecnologica[391].

Nell'EHDS l'uso primario concerne, ex art. 2, par. 2, lett. d), del Regolamento, il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso. Per quanto riguarda la circolazione dei dati sanitari primari, la normativa rafforza i diritti delle persone fisiche in relazione ai propri dati sanitari elettronici. Ciò si realizza innanzitutto mediante il riconoscimento di un diritto di accesso gratuito e in formato leggibile ai dati elettronici, esercitabile immediatamente dopo la loro registrazione in un sistema di cartelle cliniche elettroniche. Parallelamente, viene previsto il diritto di scaricare gratuitamente una copia elettronica di tali dati.

Altri diritti, in parte mutuati dal GDPR, sono declinati specificamente con riferimento ai dati sanitari elettronici, con l'intenzione di bilanciare l'obiettivo della massima condivisione delle informazioni con la necessità di garantire il pieno controllo da parte dell'interessato. Tra questi figurano il diritto di rettifica, il diritto di inserire informazioni nella propria cartella clinica elettronica, il diritto alla portabilità dei dati, il diritto di limitare l'accesso e il diritto di ottenere informazioni sulle modalità di accesso ai dati.

In particolare, l'accesso e il diritto di copia riguardano almeno le cosiddette categorie prioritarie dei dati sanitari elettronici personali, tra cui: profili sanitari sintetici dei pazienti, ricette elettroniche, dispensazioni elettroniche, esami diagnostici per immagini con relativi referti, risultati di

[391] M. MAGGIOLINI, *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitari*, in *Amministrativ@mente - Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2025, 1, 398.

laboratorio e altri esami diagnostici, nonché lettere di dimissione. L'elenco dettagliato è definito in un allegato al Regolamento, che la Commissione europea può aggiornare periodicamente, in linea con la prassi comune agli atti della cosiddetta società digitale[392].

Il GDPR, come già ricordato, ha introdotto il diritto di accesso ai dati personali, che consente agli individui di ottenere informazioni sul trattamento dei propri dati e di ricevere una copia dei dati oggetto di tale trattamento. Tuttavia, questo diritto presenta alcune limitazioni. L'accesso ai dati sanitari può richiedere tempi relativamente lunghi e, in alcuni casi, le informazioni vengono fornite esclusivamente in formato cartaceo, meno pratico per ulteriori utilizzi. Inoltre, poiché il diritto regolamenta esclusivamente la ricezione di "una copia dei dati personali oggetto di trattamento" e non disciplina esplicitamente l'accesso ai documenti medici, alcuni Stati membri, come la Svezia, richiedono il pagamento di un contributo quando vengono richiesti referti o cartelle cliniche. L'EHDS mira a superare queste difficoltà, riconoscendo agli individui un diritto chiaro e immediato di accesso ai propri dati sanitari elettronici, trattati nell'ambito dell'uso primario, senza alcun costo e in un formato facilmente fruibile. Inoltre, quest'ultimo consente ai pazienti di ricevere una copia elettronica dei propri dati sanitari, facilitando così il controllo diretto sulle informazioni personali e la loro gestione[393]. Il nuovo Regolamento introduce, in favore dell'interessato, un diritto di accesso immediato e gratuito ai propri dati sanitari, che devono essere messi a disposizione in un formato facilmente leggibile e interoperabile, consentendo altresì il download in un modello armonizzato a livello europeo (art. 3 e art. 15). Come chiarito dal Considerando 9, tale facoltà riguarda specificamente i dati in formato elettronico, senza incidere sulle ulteriori modalità di accesso

[392] M. OROFINO, *One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in *Corti Supreme e Salute*, 2025, 1, 1-19.
[393] D. FÅHRÆUS, J. REICHEL, S. SLOKENBERGA, *The European Health Data Space: Challenges and Opportunities*, Stockholm, Sieps, 2024, 5-6.

previste dal diritto generale alla protezione dei dati personali, ad esempio la possibilità di ottenere una copia cartacea ai sensi della disciplina generale.

Il diritto di accesso, tuttavia, non ha carattere assoluto[394]: il legislatore ammette la possibilità, a livello nazionale, di introdurre limitazioni motivate da esigenze di tutela della persona fisica, con particolare riferimento alla sicurezza individuale e a considerazioni di natura etica[395]. In tale prospettiva, può essere previsto un differimento temporaneo dell'accesso ai dati sanitari elettronici, al fine di consentire che un professionista sanitario possa illustrarne il contenuto e il significato clinico, garantendo così una piena comprensione da parte dell'interessato (art. 3)[396]. In questa prospettiva, il diritto dell'interessato a conoscere determinate informazioni può essere

[394] Come indicato nell'art 84, gli Stati membri sono invitati a promuovere e sostenere l'alfabetizzazione sanitaria digitale e lo sviluppo delle pertinenti competenze e abilità per i pazienti. La Commissione sostiene gli Stati membri a tal fine. Le campagne o i programmi di sensibilizzazione sono intesi in particolare a informare i pazienti e il pubblico in generale in merito all'uso primario e all'uso secondario nel quadro dello spazio europeo dei dati sanitari, tra cui i diritti che ne derivano, nonché ai vantaggi, ai rischi e ai potenziali miglioramenti per la scienza e la società dell'uso primario e all'uso secondario.

[395] Un accesso tempestivo e completo dei professionisti sanitari alle cartelle cliniche dei pazienti è fondamentale per garantire la continuità dell'assistenza. Come descritto nel cons. 19 dell'EHDS, i prestatori di assistenza sanitaria, nell'accedere ai dati sanitari elettronici personali, dovrebbero applicare il principio della minimizzazione dei dati, limitandosi a consultare i dati strettamente necessari e giustificati per la prestazione di un determinato servizio. Sebbene i dettagli relativi al funzionamento della piattaforma MyHealth@EU, destinata a favorire l'uso primario dei dati sanitari elettronici, siano ancora in fase di definizione, è già previsto che i pazienti possano esercitare un controllo selettivo sulla visibilità di parti della propria cartella clinica, modulandone l'accesso in base al tipo di professionista sanitario coinvolto. Ciò significa, ad esempio, che un individuo potrebbe consentire al proprio psichiatra di consultare i dati inerenti alla salute mentale, negandone invece l'accesso al proprio dentista. Tanto il Parlamento europeo quanto la Commissione condividono l'orientamento volto a garantire al paziente un effettivo potere decisionale nella gestione delle informazioni sensibili. Il fatto che una persona fisica abbia imposto una limitazione a norma del primo comma non è visibile ai prestatori di assistenza sanitaria. (art. 8). Tale profilo tocca un delicato equilibrio tra il diritto all'autodeterminazione informativa del soggetto interessato e l'esigenza del medico di poter operare con un quadro clinico quanto più possibile completo e attendibile. M. RYAN, P. GÜRTLER, A. BOGUCKI, *Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces*, in *International Journal of Law and Information Technology*, 2024, 32, 20-21.

[396] C. SARRA, *Il diritto alla salute nell'era della datificazione*, in *Diritto alla salute, protezione dei dati personali e intelligenza artificiale*, a cura di C. SARRA, A. ZILIO, G. DE BONA, FrancoAngeli, Milano, 2025, 31-33.

temporaneamente limitato in funzione della tutela del suo stesso benessere, così che la presa di coscienza avvenga in un contesto deontologicamente corretto e rispettoso della persona malata. Ne deriva che il momento in cui il paziente può visualizzare i propri dati non coincide necessariamente, sotto il profilo temporale, con quello in cui tali informazioni vengono registrate o caricate nel sistema informatico sanitario. Tale restrizione, di natura eccezionale e circoscritta, trova fondamento nell'art. 23 del Regolamento (UE) 2016/679 (GDPR), che consente di limitare alcuni diritti dell'interessato qualora ciò risulti necessario e proporzionato alla salvaguardia della sua tutela, purché sia garantito il rispetto dell'essenza dei diritti fondamentali e dei principi propri di una società democratica. La possibilità di limitare l'accesso ai dati sanitari elettronici non riguarda soltanto il paziente ma può operare anche in senso inverso, su iniziativa dello stesso interessato. L'art. 8 del Regolamento prevede infatti che ogni persona possa decidere di oscurare, in tutto o in parte, i propri dati sanitari elettronici personali. Tale facoltà può essere esercitata solo dopo che il paziente sia stato adeguatamente informato sulle potenziali conseguenze negative di questa scelta, in particolare in merito all'impatto che essa può avere sulla qualità dell'assistenza, sull'efficacia della prestazione sanitaria e, in ultima analisi, sulla sua stessa sicurezza e integrità psico-fisica. Il rifiuto del paziente di rendere visibili i propri dati può considerarsi giuridicamente valido solo in seguito ad aver ricevuto tali informazioni, comportando l'assunzione di responsabilità per l'eventuale impossibilità, da parte del medico, di basare le proprie valutazioni e decisioni su un quadro informativo completo. Inoltre, il Regolamento lascia agli Stati membri la possibilità di introdurre specifiche disposizioni interne volte a disciplinare la responsabilità professionale dei sanitari nei casi in cui l'accesso ai dati sia stato limitato per volontà del paziente. Tali restrizioni

dovranno essere tenute in debito conto anche in sede giudiziale, qualora si debba valutare la condotta del professionista[397].

Accanto al diritto di accedere ai propri dati e di conoscere le informazioni relative agli accessi effettuati dai prestatori di servizi sanitari (art. 9), il Regolamento riconosce agli interessati anche la possibilità di intervenire direttamente sui propri dati, integrandoli o aggiungendone di nuovi su base volontaria. Tuttavia, poiché tali modifiche non sono soggette alla supervisione di un professionista sanitario, il legislatore impone che i dati immessi dall'interessato siano chiaramente distinti da quelli generati o validati dai soggetti sanitari competenti (art. 5). I servizi di accesso ai dati sanitari elettronici, disciplinati dall'articolo 4 del Regolamento, riconoscono alle persone fisiche la possibilità di richiedere agevolmente, anche per via telematica, la rettifica dei propri dati sanitari personali, in conformità a quanto previsto dall'articolo 16 del GDPR. Tale facoltà si inserisce nel più ampio quadro dei diritti di controllo dell'interessato sui propri dati, garantendo l'aggiornamento e l'esattezza delle informazioni sanitarie. Qualora la richiesta di rettifica lo richieda, il titolare del trattamento è tenuto a verificarne la fondatezza in collaborazione con un professionista sanitario competente, al fine di assicurare la correttezza e l'affidabilità clinica dei dati oggetto di modifica (art. 6).

L'interessato dispone, inoltre, del diritto alla portabilità dei propri dati sanitari, che si concretizza nella facoltà di richiederne il trasferimento verso un'altra struttura sanitaria, un servizio sociale o un ente di rimborso, senza oneri e senza ingiustificati ritardi. Tale trasferimento può avvenire anche oltre i confini nazionali, grazie all'utilizzo dell'infrastruttura transfrontaliera e del formato europeo di scambio delle cartelle cliniche elettroniche, come previsto dall'articolo 7 del Regolamento.

---

[397] S. CACACE, *Autodeterminazione, paternalismo e responsabilità: l'uso primario dei dati sanitari nella relazione di cura e di fiducia fra medico e paziente*, in *Responsabilità Medica*, 2025, 3, 334-340.

Per realizzare l'obiettivo dello scambio di dati sanitari tra gli Stati membri dell'Unione europea e dello Spazio economico europeo, il Regolamento sull'EHDS prevede l'istituzione della piattaforma centrale *MyHealth@EU*, alla quale saranno interconnessi i sistemi sanitari nazionali (art. 12). L'infrastruttura è concepita per garantire uno scambio sicuro delle informazioni, rafforzando al contempo la tutela dei pazienti e il livello complessivo dell'assistenza sanitaria. La piattaforma non si limita a rendere possibile lo scambio di dati previsto dall'articolo 5 del Regolamento, ma facilita anche l'erogazione di servizi complementari, quali la telemedicina, la *mobile health*, l'accesso diretto dei cittadini ai propri dati e la conservazione e verifica dei certificati sanitari e vaccinali. Essa si sviluppa dall'esigenza, emersa in particolare durante la pandemia, di disporre di strumenti idonei a verificare la validità dei documenti sanitari, come nel caso dei certificati digitali europei relativi al COVID-19. In questa prospettiva, *MyHealth@EU* contribuisce alla protezione sia della salute individuale, specie nei casi di maggiore esposizione al rischio, sia della salute pubblica nel suo complesso[398].

La piattaforma è frutto di sviluppi avviati già nel 2008 con il progetto pilota epSOS (Smart Open Services for European Patients). Tale infrastruttura è destinata a garantire la circolazione transfrontaliera dei dati sanitari tra gli Stati membri, attraverso l'adozione di un formato comune armonizzato. Sia le autorità nazionali sia i prestatori di servizi sanitari saranno tenuti a connettersi a questa piattaforma, al fine di assicurare un'effettiva interoperabilità. Le specifiche tecniche necessarie saranno definite tramite atti di esecuzione, i quali disciplineranno non solo gli standard relativi al formato dei dati, ma anche i requisiti in materia di cibersicurezza, interoperabilità

[398] K. KOTSARELI, P. TSACHOURIDIS, *European Health Data Space: A New Era in EU Health*, in *HAPSc Policy Briefs Series*, 2023, 4, 2, 91-96.

tecnica e semantica, nonché le regole di gestione e funzionamento del servizio[399].

Attualmente, nell'ambito dell'Unione europea, sono in corso di progressiva attuazione due servizi sanitari digitali transfrontalieri, disciplinati e coordinati a livello sovranazionale: *l'ePrescription/eDispensation* e il *Patient Summary*.

Il primo servizio consente al cittadino europeo di ottenere i medicinali prescritti presso una farmacia situata in un diverso Stato membro, mediante il trasferimento telematico della prescrizione elettronica dal Paese di affiliazione a quello di soggiorno. Tale meccanismo, fondato sulle *Linee guida della eHealth Network in materia di ePrescription*[400] e sui relativi atti di aggiornamento, realizza un passo significativo in direzione della libera circolazione delle persone, assicurando al contempo la continuità delle cure.

Il secondo strumento, rappresentato dal *Patient Summary* digitale[401], raccoglie informazioni sanitarie essenziali – quali allergie, terapie in corso, patologie pregresse, interventi chirurgici – e costituisce parte integrante della più ampia categoria della cartella clinica elettronica (Electronic Health Record, EHR). La finalità del *Patient Summary* è quella di garantire al professionista sanitario dello Stato ospitante l'accesso, nella propria lingua, ai dati essenziali del paziente proveniente da un altro Stato membro, superando così ostacoli di natura linguistica e tecnico-organizzativa.

In una prospettiva di lungo periodo, il quadro normativo europeo (oggi progressivamente convergente nell'European Health Data Space – EHDS) prevede l'estensione dei servizi di interoperabilità transfrontaliera ad ulteriori

---

[399] J. TAMBA, *Interopérabilité des dossiers médicaux: ce qui change avec l'espace européen des données de santé*, in *Journal de droit de la santé et de l'assurance maladie*, 2025, 43, 131-138.

[400] eHealth Network, *Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU: ePrescription and eDispensation of authorised medicinal products (Release 3.1)*, novembre 2024.

[401] eHealth Network, *Guidelines on Patient Summary, Release 3.4. Guideline on the electronic exchange of health data under Cross-Border Directive 2011/24/EU: Patient Summary*, novembre 2024.

tipologie di dati clinici: immagini diagnostiche, referti di laboratorio e lettere di dimissione ospedaliera. L'obiettivo dichiarato è quello di giungere, in maniera graduale e coordinata, alla circolazione dell'intera cartella clinica elettronica a livello unionale. Giova sottolineare che lo scambio di *ePrescription* ed il *Patient Summary* costituiscono già oggi servizi aperti a tutti gli Stati membri, pur con differenti gradi di implementazione nazionale[402]. Tuttavia, come indicato dall'art. 48, l'interoperabilità delle applicazioni per il benessere con i sistemi di cartella clinica elettronica non comporta, di per sé, la condivisione automatica o la trasmissione integrale dei dati ivi contenuti. Tale condivisione o trasmissione è ammessa unicamente se conforme all'articolo 5, previo consenso espresso della persona interessata, e resta circoscritta ai fini per i quali l'interoperabilità è prevista. I produttori delle applicazioni per il benessere che dichiarano la compatibilità con i sistemi di cartella clinica elettronica sono tenuti a garantire che l'interessato possa selezionare, in maniera consapevole, le categorie di dati sanitari da inserire nel sistema nonché le modalità e le condizioni della loro eventuale trasmissione o condivisione.

In linea generale, per quanto riguarda il consenso, la possibilità di opt-out è stabilita direttamente dal legislatore europeo nel caso del trattamento per finalità secondarie, mentre per il trattamento per finalità primarie essa è prevista solo se introdotta dai singoli Stati membri (art. 10). Questo enunciato non comporta la negazione di un controllo dell'interessato sui propri dati, il quale è assicurato tramite il riconoscimento di vari diritti tra cui quelli di accesso, di rettifica e di limitazione citati. Per quanto riguarda l'uso secondario dei dati sanitari, la tutela viene offerta dal divieto di utilizzare i dati per determinate finalità (in particolare, per adottare decisioni pregiudizievoli per una persona fisica o per un gruppo di persone fisiche, per

[402] European Commission, *Electronic cross-border health services*, *Health.Europa*, 8 agosto 2025, https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en, consultato da ultimo il 7.11.2025.

svolgere attività pubblicitarie o di marketing, per sviluppare beni o servizi che possano danneggiare le persone, la salute pubblica o la società in generale e per attività contrarie all'ordine pubblico, come descritto nell'art. 54) e dalle modalità con cui la condivisione deve essere attuata, sempre intermediata da un organismo pubblico. Vi è un unico caso in cui si prevede la necessità dell'opt-in dell'interessato, quello già citato che coincide con l'utilizzo per finalità secondarie dei dati raccolti tramite le applicazioni per il benessere, considerata l'invasività di tale raccolta rispetto alla sfera privata delle persone[403].

4.4 Il riutilizzo dei dati sanitari per uso secondario

Nella governance dei sistemi sanitari si registra un crescente interesse per le fonti di dati "*real world*", considerate complementari rispetto a quelli sperimentali. Tale esigenza nasce dalla necessità di valutare gli effetti di nuovi farmaci e tecnologie non solo in condizioni controllate, ma anche nel contesto della pratica clinica quotidiana, così da confermare o integrare i processi di decision-making in ambito medico-scientifico. In questa prospettiva, strumenti quali studi osservazionali, trial pragmatici, database amministrativi, registri, cartelle cliniche elettroniche e indagini survey assumono un ruolo centrale nella raccolta e nell'analisi dei dati[404]. L'attività di ricerca medica, al pari di qualsiasi altra forma di ricerca scientifica, implica necessariamente la raccolta, l'utilizzo, la trasmissione, la condivisione e la conservazione di dati. Ciò impone a promotori, centri di ricerca, università e ricercatori di assicurare una gestione dei dati improntata a responsabilità,

[403] S. THOBANI, *Il consenso nella regolazione della circolazione dei dati*, in *Persona e Mercato*, 2025, 2, 469-486.
[404] S. SOMMARIVA *et al.*, *I registri in sanità e la creazione di conoscenza: dai database alla produzione scientifica*, in *Politiche Sanitarie*, 2015, 16(3), 168-176.

trasparenza e correttezza, garantendo al contempo un accesso appropriato e una circolazione efficace delle informazioni scientifiche[405].

È opportuno evidenziare come i dati presentino una duplice dimensione: un volto statico, rappresentato dalla loro raccolta e conservazione, e un volto dinamico, che si manifesta attraverso le molteplici attività connesse al loro utilizzo. Non è soltanto il singolo dato digitale, infatti, ad assumere rilievo, grazie a modalità di accesso e di gestione sempre più semplificate; è piuttosto l'insieme dei dati a costituire un patrimonio conoscitivo e informativo di primaria importanza, anche per finalità di interesse pubblico.

Le informazioni così generate, trascendendo l'interesse individuale, si configurano come un bene collettivo, funzionale alla soddisfazione di esigenze eterogenee: dalla partecipazione democratica dei cittadini alla formazione dell'opinione pubblica, dallo studio e dalla ricerca scientifica al miglioramento dei servizi e al supporto dei processi decisionali[406].

L'impiego secondario dei dati sanitari può riguardare una molteplicità di finalità e la possibilità di perseguire tali scopi dipende, tuttavia, in larga misura dalla disponibilità degli individui a condividere le proprie informazioni sanitarie. Un passaggio significativo in questa direzione si è avuto già nel 2002, con l'adozione da parte della World Medical Association della *Declaration on Ethical Considerations regarding Health Databases*, che ha riconosciuto l'importanza delle banche dati sanitarie per la ricerca, la garanzia della qualità e la gestione del rischio. Tale riconoscimento ha

[405] P. AURUCCI, F. DI TANO, *Dati personali e ricerca medica: condizioni, incoerenze e prospettive giuridiche a fronte dell'evoluzione interpretativa e applicativa del Garante per la protezione dei dati personali*, in *Biolaw Journal*, 2024, 3, 305-327.
[406] M. MAGGIOLINI, *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitari*, in *Amministrativ@mente - Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2025, 1, 386-401.

contribuito a consolidare la domanda di utilizzo dei dati sanitari per finalità ulteriori rispetto alla mera relazione con il personale sanitario[407].

Uno dei tratti qualificanti della disciplina dell'European Health Data Space (EHDS) è rappresentato dalla previsione di un obbligo, in capo ai soggetti che detengono dati sanitari, di condividerli per finalità diverse da quelle strettamente cliniche, purché siano rispettate le condizioni fissate dal legislatore europeo. Tale scelta normativa evidenzia la volontà dell'Unione di superare la logica meramente volontaristica nella circolazione dei dati, istituendo un regime che riconosce alla dimensione collettiva della ricerca e dell'innovazione un valore giuridicamente protetto.

Il meccanismo delineato consente a soggetti pubblici e privati (individuati genericamente come *data users*) di presentare richiesta di accesso ai titolari dei dati (*data holders*), che possono essere istituzioni sanitarie, enti di ricerca, ma anche altri organismi operanti nel settore della cura o della salute. Sebbene la condivisione costituisca un vero e proprio obbligo legale, la normativa ammette la possibilità di subordinare l'accesso al pagamento di tariffe commisurate ai costi di gestione e di predisposizione dei dataset.

Particolarmente significativo è l'ampio perimetro oggettivo definito dall'EHDS: non soltanto dati clinici in senso stretto, ma anche informazioni di carattere genetico, socio-economico, ambientale o amministrativo, che possono assumere rilievo ai fini della ricerca scientifica e della definizione di politiche sanitarie. Il riuso dei dati è infatti legittimato per finalità di interesse pubblico quali l'elaborazione di politiche sanitarie, l'addestramento di algoritmi[408], lo sviluppo di terapie personalizzate e più in generale il sostegno

---

[407] F. CASCINI *et al.*, *Health data sharing: attitudes towards primary and secondary use of data. A systematic review*, in *EClinicalMedicine*, 2024, 2-4.

[408] A tal riguardo, il considerando 61 indica: "*Le attività correlate alla ricerca scientifica comprendono le attività di innovazione quali l'addestramento di algoritmi di intelligenza artificiale che potrebbero essere utilizzati nell'assistenza sanitaria o nella cura delle persone fisiche, nonché la valutazione e l'ulteriore sviluppo di algoritmi e prodotti esistenti a tali fini. È necessario che lo spazio europeo dei dati sanitari contribuisca anche alla ricerca fondamentale e, sebbene i suoi benefici per gli utilizzatori finali e i pazienti possano risultare meno diretti, tale ricerca è fondamentale per i benefici per la società a lungo termine*."

all'innovazione medica. A garanzia degli interessati, l'accesso è mediato dagli *Health Data Access Bodies*, chiamati a bilanciare l'esigenza di apertura con la tutela dei diritti fondamentali, in particolare del diritto alla protezione dei dati personali[409]. Il Regolamento EHDS non stabilisce restrizioni su chi possa richiedere l'accesso ai dati per uso secondario: qualsiasi persona fisica o giuridica può presentare una domanda di accesso ai dati (art. 50). L'autorizzazione all'accesso viene concessa dall'organismo competente per l'accesso ai dati sanitari, a condizione che la richiesta rientri tra gli scopi consentiti (art. 52) e che i soggetti autorizzati possano accedere e trattare i dati sanitari elettronici esclusivamente secondo quanto previsto dal permesso rilasciato e rispettando le condizioni stabilite, tra cui il divieto di re-identificare, o tentare di re-identificare, le persone da cui i dati sono stati estratti (art. 54).

Un ulteriore obbligo per gli utenti dei dati consiste nella pubblicazione dei risultati della ricerca derivante dall'utilizzo dei dati entro 18 mesi dal completamento del trattamento dei dati sanitari elettronici o dalla ricezione della risposta alla richiesta di accesso (art. 68-69). L'accesso ai dati avviene tramite l'intermediazione dell'organismo per l'accesso ai dati sanitari, che può rilasciare il permesso e successivamente richiedere i dati ai detentori degli stessi; i dati devono essere messi a disposizione dell'utente entro tre mesi dal momento in cui vengono ricevuti dai detentori (art. 53). La durata del permesso di accesso ai dati deve essere limitata al tempo necessario per gli scopi richiesti e, in ogni caso, non può superare i dieci anni (art. 68)[410].

Negli ultimi anni l'evoluzione tecnologica ha determinato l'emergere di nuove fonti di dati sanitari, che si affiancano ai tradizionali strumenti di documentazione clinica. Internet, dispositivi indossabili, applicazioni mobili,

---

[409] S. VAN DRUMPT et al., *Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies*, in *Frontiers in Digital Health*, 2025, 7, 2-3.

[410] I. LIANOS, *Access to Health Data, Competition, and Regulatory Alternatives: Three Dimensions of Fairness*, in *Journal of Competition Law & Economics*, 2025, 44-46.

cartelle cliniche elettroniche e tecniche di sequenziamento genomico consentono infatti la raccolta e la gestione di informazioni sempre più puntuali e personalizzate. Queste fonti, se utilizzate correttamente, offrono opportunità rilevanti per la ricerca, la sanità pubblica e lo sviluppo di politiche sanitarie basate sui dati[411]. Si pensi ad esempio alla IoMT – *Internet of Medical Things*, che tratta l'insieme di dispositivi connessi alla rete che trasmettono e raccolgono dati sanitari in tempo reale (per l'appunto wearable devices, sensori biometrici, monitor e strumenti che permettono di monitorare in maniera continua le condizioni di salute dei pazienti). L'effetto di tali strumenti è quello di ridurre le visite ospedaliere e di migliorare la gestione delle patologie croniche[412]. La seguente tabella riporta le principali fonti emergenti di dati sanitari e loro applicazioni (sebbene la sintesi non abbia pretesa di esaustività).

Tabella 7 Fonti emergenti di dati sanitari e le loro applicazioni.

Fonte di dati	**Descrizione**	**Esempi e applicazioni**
Internet e social media	Generano dati sanitari indiretti attraverso comportamenti digitali (ricerche online, interazioni social). Offrono informazioni tempestive e ad alta risoluzione territoriale.	Query dei motori di ricerca, contenuti e interazioni sui social network, articoli delle testate online. Utili per attività di *epidemic intelligence* e per il monitoraggio delle tendenze sanitarie.

[411] A. F. NÄHER *et al.*, *Secondary data for global health digitalisation*, in *The Lancet Digital Health*, 2023, 5(2), 93-101.
[412] M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari – Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Santarcangelo di Romagna, Maggioli Editore, 2025.

Dispositivi indossabili e applicazioni mobili	Producono ingenti quantità di dati personalizzati, relativi sia a parametri fisiologici sia a condizioni mediche generali. Consentono un monitoraggio continuo e in tempo reale.	Smartwatch, FitBit, Oura ring; app come *Corona Data Donation* per il tracciamento del COVID-19 (frequenza cardiaca, temperatura corporea, attività fisica, sonno). *Symptom checkers* (Ada, Your.MD) per valutazioni preliminari e autodiagnosi.
Cartelle cliniche elettroniche (EHR)	Sistemi digitali che raccolgono e integrano dati clinici nel percorso assistenziale e di cura.	Referti medici, dati demografici, indicatori socioeconomici. Esempi: moduli di sorveglianza per tubercolosi, algoritmi per determinare profilassi pre-esposizione all'HIV, influenza e diabete. Persistono criticità legate a ostacoli organizzativi, tecnici e gestionali.
Sequenziamento genomico	Fornisce informazioni molecolari sui genomi, rilevanti per diagnosi	Varianti SARS-CoV-2, stime di incidenza COVID-19,

	personalizzate e per la definizione di politiche sanitarie. Consente il tracciamento della diffusione di varianti e ceppi resistenti e di fare uno screening della popolazione.	localizzazione di tubercolosi resistente, stima delle infezioni recenti HIV/HCV, epidemie di origine alimentare. Banche dati: *GenBank*, *Sequence Read Archive*, *GISAID*, *European Nucleotide Archive*.

In questo contesto è particolarmente interessante la definizione di "applicazione per il benessere": fornita dall'art. 2 dell'EHDS, che sintetizza dispositivi indossabili e applicazioni relative al monitoraggio della salute come qualsiasi software o combinazione di hardware e software, destinati dal fabbricante a essere utilizzati da una persona fisica, per il trattamento dei dati sanitari elettronici, specificamente per fornire informazioni sulla salute di una persona fisica o per fornire cure assistenziali per scopi diversi dalla prestazione di assistenza sanitaria.

L'estensione e l'intensificazione dei sistemi informativi che trattano dati legati alla salute, unitamente alla diffusione di archivi digitali sempre più capienti ed efficienti, aprono prospettive significative per il progresso medico e farmacologico e per il miglioramento delle prestazioni assistenziali. Tuttavia, a queste potenzialità si affiancano nuove sfide di natura giuridica ed etica[413]. Fra esse spicca il nodo della riservatezza dei dati sanitari, ambito nel

[413] Per garantire la necessaria dimensione campionaria e un'adeguata rappresentatività delle popolazioni cliniche, la ricerca in ambito biomedico ricorre frequentemente al modello degli studi multicentrici, in particolare quando si utilizzano approcci statistici o metodologie di apprendimento automatico. Tali studi, per loro natura, implicano il trattamento di dati sanitari, genetici o biometrici provenienti da fonti eterogenee, gestiti da una pluralità di

quale si innesta una tensione costante tra la salvaguardia delle prerogative individuali e la tutela di interessi di carattere collettivo. È proprio in tali contesti, segnati dalla ricerca di un equilibrio tra diritti della persona e finalità pubbliche, che emergono con maggiore evidenza le complessità e le ambivalenze generate dall'uso esteso delle informazioni sanitarie[414].

Il GDPR non utilizza espressamente la nozione di *secondary use* dei dati, ma fa riferimento al concetto di *ulteriore trattamento* (*further processing*). Pur non essendo definito in maniera puntuale, dal considerando 50 si evince che tale espressione designi il trattamento di dati personali per finalità diverse da quelle per le quali i dati sono stati originariamente raccolti. La qualificazione di un determinato utilizzo secondario come ulteriore trattamento ai sensi del GDPR riveste rilievo centrale, poiché incide direttamente sulla ripartizione dei ruoli e delle responsabilità tra i soggetti coinvolti nel trattamento.

Il principio di limitazione delle finalità, sancito dall'art. 5, par. 1, lett. b), GDPR, stabilisce in via generale che i dati personali debbano essere raccolti per finalità determinate, esplicite e legittime e non possano essere ulteriormente trattati in modo incompatibile con tali finalità. A tale regola si accompagnano due eccezioni rilevanti: l'ulteriore trattamento è ammesso quando fondato sul consenso dell'interessato oppure quando è previsto dal diritto dell'Unione o degli Stati membri come misura necessaria e

soggetti e oggetto di condivisione a più livelli. L'ampiezza e la complessità dei dataset coinvolti sollevano, tuttavia, rilevanti problematiche giuridiche. Tra queste si annoverano: la qualificazione dei dati personali trattati, l'individuazione dei ruoli e delle responsabilità dei soggetti partecipanti al trattamento, l'identificazione delle basi giuridiche che ne legittimano l'utilizzo, nonché la regolamentazione e l'adeguamento dei flussi informativi, inclusi quelli che comportano trasferimenti di dati a livello transnazionale. F. DI TANO, *Studi multicentrici, ruoli privacy e flussi di dati UE ed extra UE*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future: atti del convegno, Trento, 28 settembre 2023*, Trento, Università degli Studi di Trento, 2024, 39-56.

[414] F. DI CIOMMO, *Trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e Responsabilità*, 2002, 2, 121-134.

proporzionata, in una società democratica, alla tutela di rilevanti interessi pubblici (art. 6, par. 4, e considerando 50 GDPR).

Inoltre, il GDPR riconosce espressamente la compatibilità dell'ulteriore trattamento dei dati per finalità di archiviazione nel pubblico interesse, ricerca scientifica o storica e fini statistici, purché svolto nel rispetto delle garanzie previste dall'art. 89, par. 1[415].

Per garantire la conformità di un progetto di ricerca in ambito medico, biomedico o epidemiologico alla normativa sulla protezione dei dati personali, è essenziale che la pianificazione tenga conto fin dall'inizio (nella fase di definizione della tipologia di studio e di redazione del protocollo con la relativa documentazione) degli obblighi derivanti dal quadro regolatorio vigente.

In Italia, i principali riferimenti normativi sono costituiti dal Regolamento (UE) 2016/679 (GDPR), come appena discusso, e dal d.lgs. 30 giugno 2003, n. 196 (Codice Privacy), come successivamente modificato per adeguarsi alla disciplina europea. A livello nazionale, un ruolo centrale è svolto dal Garante per la protezione dei dati personali, che ha emanato, tra l'altro, le prescrizioni relative al trattamento dei dati genetici (Aut. gen. n. 8/2016)[416] e quelle concernenti l'utilizzo dei dati personali per finalità di ricerca scientifica (Aut. gen. n. 9/2016)[417].

Sul piano europeo, ulteriori indicazioni interpretative e di indirizzo sono contenute nella *Preliminary Opinion on data protection and scientific research* pubblicata dall'European Data Protection Supervisor (EDPS) nel 2020, nonché nel documento dell'European Data Protection Board (EDPB)

---

[415] R. BECKER *et al.*, *Secondary use of personal health data: when is it "further processing" under the GDPR, and what are the implications for data controllers?*, in *European Journal of Health Law*, 2022, 30(2), 129-157.

[416] Garante per la protezione dei dati personali. *Prescrizioni relative al trattamento dei dati genetici.* Autorizzazione generale n. 8/2016.

[417] Garante per la protezione dei dati personali. *Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica.* Autorizzazione generale n. 9/2016.

volto a chiarire i profili di applicazione uniforme del GDPR in materia di ricerca sanitaria[418].

Nell'ambito delle attività di ricerca sanitaria, la tutela dei dati personali e la salvaguardia della riservatezza assumono come affermato un rilievo centrale, tanto più in ragione della particolare delicatezza delle informazioni trattate. Per tale motivo, accanto alla documentazione di natura scientifica, risulta imprescindibile predisporre anche l'apparato documentale relativo alla protezione dei dati, da integrare in maniera coerente con quello tecnico-scientifico, al fine di garantire la piena conformità alle disposizioni normative vigenti in materia. In determinate ipotesi, come nel caso dell'informativa sul trattamento e dei consensi informati, gli strumenti di tutela della privacy finiscono per costituire parte sostanziale e non meramente accessoria della stessa documentazione scientifica. L'informativa privacy costituisce lo strumento attraverso il quale i soggetti coinvolti in una ricerca vengono messi a conoscenza, in maniera chiara e completa, delle modalità di trattamento dei propri dati personali. In un'ottica di trasparenza e responsabilizzazione del titolare, essa deve riportare con precisione le finalità perseguite, le categorie di dati raccolti, i soggetti destinatari, le basi giuridiche del trattamento, nonché i diritti riconosciuti agli interessati e le modalità di contatto con il responsabile del trattamento per l'esercizio di tali diritti.

Accanto all'informativa, la documentazione di ricerca comprende generalmente i moduli di consenso. Essi si distinguono, da un lato, nel consenso informato, con il quale il partecipante manifesta adesione volontaria alla ricerca; dall'altro, nel consenso al trattamento dei dati personali[419],

---

[418] G. BINCOLETTO, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina: la tutela dei dati personali tra regole e prassi*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, Trento, Università degli Studi di Trento, 2024, 105-125.

[419] Nel settore della ricerca scientifica, l'utilizzo secondario dei dati non risulta automaticamente contrario al principio generale di limitazione delle finalità del trattamento, come previsto dall'articolo 5, par. 1, lett. b) del GDPR, grazie alla presunzione di compatibilità ivi stabilita. Tuttavia, tale trattamento è ammesso esclusivamente se supportato da una solida base giuridica che ne legittimi la conduzione.

mediante il quale l'interessato autorizza l'utilizzo delle proprie informazioni per le finalità specifiche indicate nello studio.

Sia l'informativa sia i consensi, unitamente al protocollo di ricerca, costituiscono parte integrante del corredo documentale che fonda la legittimità dell'indagine. Il linguaggio utilizzato deve contemperare due esigenze: da un lato, risultare comprensibile e accessibile per i partecipanti; dall'altro, mantenere coerenza con il quadro tecnico-scientifico delineato dal protocollo. In questo contesto, gli accordi di titolarità rappresentano strumenti giuridici volti a definire, all'interno di un progetto di ricerca, la ripartizione delle funzioni e delle responsabilità connesse al trattamento dei dati personali. Essi precisano il ruolo dei soggetti coinvolti – individuando chi assume la qualità di titolare del trattamento e chi quella di responsabile – nonché le modalità con cui i dati sono gestiti e condivisi tra le diverse istituzioni partecipanti. In tal modo, tali accordi assicurano chiarezza rispetto agli obblighi derivanti dal quadro normativo e garantiscono una corretta allocazione delle competenze tra i vari attori della ricerca. Inoltre, parte integrante della documentazione relativa alla componente di trattamento dei dati è la valutazione d'impatto sulla protezione dei dati[420].

Il GDPR stabilisce requisiti specifici che devono essere presenti in tutti gli accordi di contitolarità del trattamento. Questi ultimi si realizzano quando ad esempio più centri di ricerca lavorano in maniera congiunta. Tali accordi devono:

- Riflettere in modo chiaro i ruoli e i rapporti tra i corresponsabili del trattamento nei confronti degli interessati, assicurando la tutela dei diritti e delle libertà di questi ultimi;
- Prevedere la possibilità di designare un unico punto di contatto per i partecipanti alla ricerca scientifica;

[420] L. GIOS, *Strutturazione e gestione di una iniziativa di ricerca. Dallo sviluppo della documentazione alla gestione del dato*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, Trento, Università degli Studi di Trento, 2024, 21-38.

- Attribuire in maniera inequivocabile responsabilità e compiti sia ai corresponsabili del trattamento sia agli incaricati del trattamento, in conformità con le disposizioni del GDPR.

L'essenza dell'accordo deve essere resa disponibile agli interessati, in modo che sia trasparente la distribuzione del controllo e della gestione dei dati.

A livello nazionale, esempi di regolamentazione in materia sono forniti, tra gli altri, dalla legge norvegese n. 38 del 15 giugno 2018 e dalla legge belga del 30 luglio 2018 (*Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*).

In base all'art. 26 del GDPR, le clausole dell'accordo devono specificare l'esercizio dei diritti degli interessati e l'obbligo dei corresponsabili di fornire tutte le informazioni previste dagli articoli 13 e 14 del GDPR. L'articolo 26 richiede inoltre di definire chiaramente le rispettive funzioni di comunicazione, le responsabilità, gli obblighi dei titolari e degli eventuali incaricati del trattamento, nonché le modalità di interazione con le autorità di controllo, come indicato nel Considerando 79 del GDPR[421].

L'ambito di applicazione del GDPR rischia di risultare insufficiente a proteggere efficacemente i soggetti interessati rispetto alle pratiche potenzialmente dannose emergenti nello sviluppo di infrastrutture e prodotti digitali nei settori del welfare e della sanità. Tale criticità può essere analizzata alla luce di quattro tensioni principali, identificate dalla dottrina recente[422]:

---

[421] V. COLCELLI, *Circolazione internazionale e trasferimento di campioni e dati personali: analisi di alcune caratteristiche del contratto*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, Trento, Università degli Studi di Trento, 2024, 127-146.

[422] L. MAAß *et al.*, *Digital Public Health in Europe: Was the COVID-19 Pandemic an Enabler for Healthcare Digitalization?*, in *Digital Public Health - Interdisciplinary Perspectives*, a cura di H. ZEEB et al., Cham, Springer Nature Switzerland, 2024, 179-210.

- Minimizzazione dei dati vs. Big Data: i principi di limitazione della finalità e di minimizzazione dei dati sanciti dal GDPR si confrontano con la crescente necessità di raccogliere grandi volumi di informazioni per l'addestramento di algoritmi predittivi, determinando una tensione tra tutela della privacy e sviluppo tecnologico;
- Dati sensibili vs. non sensibili: l'incrocio di dataset apparentemente non sanitari (quali dati sullo stile di vita) o pseudonimizzati (ad esempio dati genetici) consente di ricostruire lo stato di salute o addirittura l'identità dei soggetti, ponendo nuove sfide in tema di protezione dei dati personali;
- Consenso attivo e informato vs. acquiescenza passiva: la complessità delle condizioni di utilizzo e le pressioni sociali o tecnologiche possono determinare un consenso prestato senza reale consapevolezza, compromettendo l'efficacia dei meccanismi di autodeterminazione informativa previsti dal GDPR;
- Potenzialità vs. rischi dell'analisi predittiva: il GDPR offre strumenti limitati per contrastare fenomeni come i *bias* algoritmici, che possono incidere negativamente sulla correttezza, trasparenza e imparzialità delle decisioni automatizzate basate sui dati.

Si ricorda che, come descritto nel cons. 53 dell'EHDS, l'uso secondario di dati sanitari elettronici si basa su dati pseudonimizzati o anonimizzati, al fine di impedire l'identificazione degli interessati. A tal proposito, gli organismi responsabili dell'accesso ai dati sanitari dovrebbero cooperare a livello transfrontaliero per sviluppare e scambiare le migliori pratiche e tecniche. Ciò include norme per la pseudonimizzazione e l'anonimizzazione di serie di microdati. Se del caso, la Commissione dovrebbe stabilire le procedure e le prescrizioni e fornire strumenti tecnici per una procedura unificata di pseudonimizzazione e anonimizzazione dei dati sanitari elettronici (cons. 65).

Considerata la particolare sensibilità dei dati sanitari elettronici, occorre ridurre al minimo i rischi per la riservatezza delle persone fisiche, in applicazione del principio di minimizzazione dei dati. Ne consegue che, ove possibile, dovrebbero essere resi disponibili esclusivamente dati sanitari elettronici non personali, qualora questi risultino sufficienti a soddisfare le finalità perseguite. Qualora, invece, l'utente necessiti di accedere a dati sanitari elettronici personali, sarà tenuto a motivare espressamente la propria richiesta, fornendo adeguata giustificazione. Spetterà, quindi, all'organismo competente per l'accesso ai dati sanitari verificare la fondatezza della motivazione addotta (cons. 72 dell'EHDS). Il Regolamento (UE) 2022/868 (Data Governance Act) disciplina in via generale l'altruismo dei dati. Tuttavia, considerata la natura particolarmente sensibile dei dati trattati in ambito sanitario, si rende necessario prevedere criteri ulteriori e più stringenti, da definirsi mediante i codici di condotta previsti dallo stesso regolamento (cons. 78 dell'EHDS).

Per mettere in sicurezza i dati sanitari non è sufficiente attivare misure volte alla protezione da attacchi informatici, è invece necessario che vengano attivate metodologie più avanzate per la protezione dei dati sia in fase di archiviazione sia in fase di trasferimento tra enti sanitari diversi ed istituti di ricerca. Tra le strategie più efficaci si considera la crittografia end-to-end che previene intercettazioni e accessi non autorizzati da parte di soggetti terzi, insieme a sistemi di autoidentificazione forti, che si basano su identificazione biometrica o chiavi crittografiche avanzate che garantiscono l'accesso solo al personale autorizzato[423].

In conclusione, la disciplina concernente l'uso secondario dei dati sanitari elettronici introduce un elemento di significativa innovazione nel panorama della regolazione europea in materia di salute e trattamento dei dati

[423] M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari – Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Santarcangelo di Romagna, Maggioli Editore, 2025.

personali. Il nuovo sistema, fondato non più sul consenso dell'interessato ma sul riconoscimento di un diritto di esclusione (*opt-out*), attribuisce alla persona fisica la facoltà di opporsi alla messa a disposizione dei propri dati per finalità diverse da quelle primarie di cura.

Questa scelta normativa segna un passaggio concettuale rilevante: da un modello centrato sull'autorizzazione individuale a uno che riconosce la dimensione pubblica e collettiva del dato sanitario, pur preservando la libertà dell'individuo di esercitare un potere di opposizione. L'approccio mira a favorire la ricerca scientifica in ambito medico e lo sviluppo della medicina di precisione, predittiva e preventiva, con potenziali effetti positivi sotto il profilo sociale e sanitario. La maggiore accessibilità dei dati, infatti, potrebbe contribuire a diagnosi più tempestive e accurate, nonché alla riduzione degli errori clinici e degli eventi avversi.

Tuttavia, gli effetti concreti di tale impianto regolatorio non saranno immediati. I tempi di attuazione risultano articolati e progressivi: per l'utilizzo secondario dei dati sanitari si prevede un periodo transitorio di almeno quattro anni dall'entrata in vigore del Regolamento, che diventa di sei anni per i dati genetici, genomici e quelli provenienti da applicazioni destinate al benessere.

Sul piano operativo, l'efficacia del nuovo sistema dipenderà in misura determinante dalla capacità degli Stati membri di predisporre un'infrastruttura tecnica e organizzativa idonea a garantire la reale disponibilità e fruibilità dei dati. Sarà necessario assicurare l'interoperabilità dei sistemi, la corretta applicazione delle tecniche di anonimizzazione e pseudonimizzazione e l'efficiente funzionamento degli organismi nazionali di accesso ai dati.

Permangono, inoltre, criticità legate all'eterogeneità delle discipline nazionali. Le differenti modalità di recepimento e implementazione del quadro europeo nei vari ordinamenti rischiano di compromettere l'obiettivo di costruire uno spazio unitario dei dati sanitari, orientato alla tutela del

pubblico interesse. In questo contesto, il diritto di esclusione riconosciuto agli individui, sebbene rappresenti una garanzia di autonomia e controllo, potrebbe non rivelarsi sufficiente a fronte di un utilizzo dei dati ancora disomogeneo sul piano interno, con il rischio di frammentare l'effettività delle tutele e di attenuare la portata innovativa del nuovo sistema[424].

[424] A. A. MOLLO, *Prime riflessioni sul Regolamento Europeo sullo spazio europeo dei dati sanitari: l'uso secondario e il diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali*, in *BioLaw Journal – Rivista di BioDiritto*, 2025, 3, 11-29.

CONCLUSIONI

Il presente lavoro di tesi è stato realizzato con l'obiettivo di offrire un contributo utile alla comprensione della solidità e dell'adeguatezza del diritto europeo in materia di dati, in un contesto caratterizzato da profondi mutamenti tecnologici. La questione risulta particolarmente significativa se consideriamo le sfide individuate dalle istituzioni europee stesse, soprattutto nell'ambito della formulazione della "Strategia Europea per i Dati". L'efficace implementazione delle iniziative strategiche poste dalla Commissione è infatti di rilevanza fondamentale non solo per garantire la coesione e la competitività dell'Unione Europea come attore internazionale, ma anche per permettere agli Stati membri, da soli incapaci di confrontarsi alla pari con potenze come gli Stati Uniti e la Repubblica Popolare Cinese, di sostenere un ruolo rilevante nel panorama globale.

L'Europa mira a conquistare quella che viene definita "sovranità digitale". Tale formula sintetizza l'obiettivo strategico di integrazione sovranazionale che punta a rafforzare il ruolo del continente nello scenario geopolitico globale. Tale ambizione risponde alla necessità di ridefinire i rapporti di forza a livello mondiale, soprattutto di fronte alla crescente competizione tecnologica. L'Unione Europea, infatti, non intende soltanto prepararsi a cogliere le opportunità offerte dal progresso tecnologico, favorendo la crescita del mercato digitale, la competitività produttiva e gli investimenti nei settori più innovativi, ma vuole anche prevenire possibili minacce ibride, ossia quei rischi che derivano dall'interdipendenza tra spazio digitale, economia e sicurezza[425]. L'Unione dovrebbe orientarsi tuttavia verso un'idea di sovranità digitale "aperta", capace di integrare anche partner esterni in grado di fornire competenze e strumenti attualmente non disponibili

[425] A. ALÙ, *La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale*, in *Rivista italiana di informatica e diritto*, 2022, 4, 251-260.

sul continente. Allo stesso tempo, è necessario investire in modo più deciso nella costruzione di un'infrastruttura digitale europea, in grado di competere efficacemente con i principali concorrenti globali[426].

La Strategia Europea per i Dati, adottata a febbraio 2020, segna un netto cambiamento rispetto all'impostazione normativa del quinquennio precedente, caratterizzata dall'entrata in vigore, nel maggio 2018, del Regolamento (UE) 2016/679, noto come GDPR. L'obiettivo fondamentale del GDPR è quello di tutelare i diritti e le libertà delle persone fisiche con riguardo al trattamento dei dati personali, creando un quadro normativo uniforme applicabile in tutti gli Stati membri dell'Unione. Al contempo esso favorisce la libera circolazione dei dati personali nel mercato interno, sotto la protezione di un solido sistema di garanzie a tutela degli interessati. Tale quadro si fonda essenzialmente sui pilastri riconducibili ai principi di trasparenza, accountability e al consenso degli interessati. La dottrina ha più volte approfondito il rapporto tra le due direttrici dell'azione dell'Unione. Il tentativo di coniugare crescita economica e tutela dei diritti fondamentali viene spesso descritto come il confronto tra due impostazioni: da un lato, una visione orientata alla funzionalità e alla competitività del mercato digitale (*market-based approach*); dall'altro, un'impostazione che pone al centro i valori e le garanzie proprie dell'ordinamento europeo (*value-based* o *rights-based approach*). Questa polarità mette in luce la sfida di integrare esigenze economiche e principi valoriali all'interno della strategia europea per il digitale[427].

Il GDPR è inoltre caratterizzato da un approccio fondato sulla gestione del rischio intrinsecamente connesso al trattamento dei dati. Il testo prevede strumenti operativi volti a prevenire possibili violazioni dei diritti

[426] S. TORREGIANI, *Il Data Act: una versione europea del Data Nationalism?*, *Rivista italiana di informatica e diritto*, 2024, 5(2), 131-146.
[427] L. PASERI, *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, Torino, Giappichelli, 2025.

degli interessati e a garantire la responsabilizzazione dei titolari e dei responsabili del trattamento.

Con la Strategia Europea per i Dati, l'accento normativo si è spostato dal concetto di rischio a quello di opportunità. Pur riconoscendo che nella nostra società la quantità di dati generati dai singoli cittadini è in costante aumento, la Commissione europea continua a sostenere che la metodologia di raccolta e utilizzo di tali dati debba porre al primo posto gli interessi delle persone, conformemente ai valori, ai diritti fondamentali e alle norme europee. Il volume crescente di dati industriali non personali e di dati pubblici in Europa, unitamente ai cambiamenti tecnologici riguardanti le modalità di conservazione ed elaborazione dei dati, deve tuttavia costituire una potenziale fonte di crescita e innovazione da valorizzare.

Di conseguenza, regolare i dati significa, da un lato, promuovere il progresso economico e sociale attraverso la piena valorizzazione degli stessi; dall'altro, preservare la centralità della persona e dei suoi diritti fondamentali all'interno del quadro normativo europeo. Questa evoluzione normativa riflette un equilibrio tra sfruttamento delle opportunità offerte dai dati e tutela dei diritti degli interessati. Tale approccio integra innovazione e protezione, ed è coerente con i principi costituzionali e comunitari di rispetto della dignità e della libertà degli individui.

Al di là della tutela dei diritti della personalità e della libertà di prestare il consenso, è innegabile che lo sviluppo di un mercato digitale dei dati possa concorrere anche alla realizzazione di interessi collettivi, in ambiti quali la sanità, la sicurezza, la ricerca scientifica e storica, nonché la protezione ambientale. In tal senso, il quarto considerando del Regolamento (UE) 2016/679 ribadisce che il trattamento dei dati personali deve porsi al servizio dell'uomo e che il diritto alla protezione dei dati personali non vada interpretato come una prerogativa assoluta, ma alla luce della sua funzione sociale, contemperandolo con altri diritti fondamentali in ossequio al principio di proporzionalità.

La cessione altruistica dei propri dati si fonda tuttavia sull'assunto che i dati costituiscano beni di rilevanza economica riferibili ad una persona, la quale può liberamente disporne nel contesto di un rapporto contrattuale con il gestore della piattaforma, cedendoli a titolo di controprestazione per l'erogazione di un servizio. Ciononostante, ciò che assume rilievo primario è il controllo esercitabile dall'interessato sulla circolazione dei propri dati [428].

Riemerge qui il tema, ormai centrale, della qualificazione giuridica dei dati. Le diverse normative che ne regolano l'utilizzo e la condivisione riportano l'attenzione su un duplice profilo: da un lato, il loro valore economico, in quanto oggetto di scambio e di rapporti patrimoniali; dall'altro, il loro valore sociale, come risorsa capace di generare benefici collettivi attraverso forme di condivisione anche "altruistica", orientate a finalità sociali, solidali o non lucrative. Si delinea così una visione più articolata del valore dei dati, che supera la semplificazione, ormai abusata, dei dati come "nuovo petrolio" dell'economia contemporanea[429].

Nella prospettiva descritta, l'impiego di approcci data-driven nei contesti territoriali appare strettamente legato alla capacità delle istituzioni di utilizzare le informazioni disponibili per migliorare la qualità delle decisioni pubbliche, dalla programmazione dei servizi alla gestione di settori particolarmente sensibili come quello sanitario.

L'esperienza dello European Health Data Space è significativa proprio perché mostra, in modo concreto, come l'uso dei dati possa diventare uno strumento di innovazione e di interesse collettivo, senza che venga meno l'esigenza di tutelare i diritti individuali. In questo ambito, le politiche basate

[428] M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Rivista italiana di informatica e diritto*, 3(2), 2021, 7-23.
[429] C. CAMARDI, *Sulla Governance digitale europea: una proposta di confronto | European digital Governance: a call for discussion*, in *Accademia. Rivista dell'Associazione dei civilisti italiani – Confronti*, 2023, 1, 7-10.

sui dati si confrontano quotidianamente con il problema del bilanciamento tra efficienza, ricerca, sicurezza e protezione della persona.

Dal lato delle imprese, il dato assume una rilevanza crescente come fattore produttivo e leva competitiva. Ne deriva la necessità di politiche data-driven attente non solo alle opportunità economiche, ma anche ai profili di rischio, alla sicurezza e alla conformità alle norme europee.

Nel complesso, il testo restituisce l'immagine di un diritto europeo dei dati che non si limita a disciplinare la circolazione delle informazioni, ma orienta in modo sostanziale le politiche pubbliche e private basate sui dati. In questo senso, l'approccio data-driven appare sostenibile solo se inserito in un quadro normativo capace di tenere insieme innovazione, sviluppo economico, interesse pubblico e tutela dei diritti fondamentali.

La proposta di Digital Omnibus del 19 novembre 2025 si inserisce nel contesto preso in esame e rappresenta un primo intervento volto a ottimizzare l'applicazione del quadro normativo digitale europeo, attraverso una serie di modifiche tecniche mirate a un ampio insieme di atti legislativi esistenti. L'obiettivo principale dell'iniziativa è quello di ridurre gli oneri di conformità per imprese, pubbliche amministrazioni e cittadini, senza pregiudicare le finalità sostanziali della regolazione, ma anzi trasformando il rispetto delle regole in un fattore di competitività per gli operatori responsabili. In questa prospettiva, la proposta mira a garantire che l'adempimento degli obblighi normativi avvenga a costi più contenuti, mantenendo inalterati i livelli di tutela e favorendo al contempo l'innovazione e la crescita del mercato digitale europeo.

Le modifiche previste sono state individuate sulla base di consultazioni con gli stakeholder e dei primi dialoghi di attuazione condotti dalla Commissione europea, in particolare sotto il coordinamento della Vicepresidente esecutiva Henna Virkkunen e del Commissario Michael McGrath. Tali interventi si concentrano in modo prioritario sullo sblocco delle potenzialità legate all'uso dei dati, considerati una risorsa strategica per

l'economia dell'Unione, anche in funzione del sostegno allo sviluppo e all'adozione di soluzioni di intelligenza artificiale affidabili nel mercato europeo. In questo quadro, le modifiche alle norme in materia di protezione dei dati personali e di tutela della privacy si inseriscono come strumenti di semplificazione immediata, volti a rafforzare la capacità di imprese e individui di esercitare i propri diritti, favorendo al contempo un utilizzo dei dati più efficiente, sicuro e coerente con i valori fondamentali dell'Unione Europea. La proposta di Digital Omnibus introduce inoltre una soluzione chiara e strutturata per razionalizzare gli obblighi di segnalazione degli incidenti di cibersicurezza, prevedendo la confluenza di tutti i relativi adempimenti all'interno di un unico meccanismo di notifica. Tale intervento è finalizzato a ridurre la frammentazione degli obblighi di reporting derivanti da diversi atti normativi, semplificando le procedure per i soggetti obbligati e migliorando, al contempo, l'efficacia e la tempestività delle comunicazioni alle autorità competenti. In questo modo, il Digital Omnibus mira a rafforzare la coerenza del quadro europeo in materia di cibersicurezza, limitando gli oneri amministrativi senza compromettere gli obiettivi di prevenzione, risposta e gestione degli incidenti[430].

In conclusione è utile soffermarsi sul ruolo dei *data centers*. I "centri di dati" costituiscono l'infrastruttura materiale che sostiene i servizi digitali e di rete: al loro interno avvengono le tanto discusse attività di conservazione, elaborazione e distribuzione delle informazioni. Su queste strutture si fondano una parte crescente dei servizi avanzati da cui dipendono le economie descritte. Nonostante essi siano elementi essenziali del funzionamento dell'ecosistema digitale, i data centers sono spesso collocati lontano dalle aree centrali e rimangono invisibili al pubblico. Questi sono

[430] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e le direttive 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557, per quanto riguarda la semplificazione del quadro legislativo digitale, e che abroga i regolamenti (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 e la direttiva (UE) 2019/1024 (*Digital Omnibus*).

complessi sistemi ad alta sicurezza che ospitano apparati sempre più imponenti destinati alla gestione dei flussi informativi generati dalle nostre attività quotidiane: messaggi di posta elettronica, contenuti multimediali, interazioni sui social network, ricerche in rete e processi che richiedono elaborazioni in tempo reale.

L'immagine evocativa della "nuvola" (*cloud*) tende tuttavia a celare la dimensione fisica di queste infrastrutture, alimentate da reti elettriche locali, gruppi elettrogeni, sistemi di accumulo e sofisticati impianti di raffreddamento. Inoltre, esse sono collegate ai principali nodi di scambio tramite dorsali in fibra ottica continentali e transoceaniche.

Il loro funzionamento richiede quantità sempre maggiori di energia, acqua, materiali rari e superfici territoriali. La problematica futura è rappresentata dalla rapidità di crescita del volume dei dati prodotti. In prospettiva di ricerca futura si segnalano questioni di governance complesse che riguardano la sostenibilità delle risorse impiegate, l'impatto territoriale e la necessità di un quadro regolatorio capace di conciliare innovazione tecnologica e tutela dell'interesse pubblico[431]. Anche l'intelligenza artificiale generativa richiede ingenti risorse computazionali per l'addestramento dei modelli e per le operazioni di elaborazione. Tuttavia, le implicazioni legate ai rifiuti elettronici (*e-waste*) derivanti da tali attività e le strategie per la loro gestione restano ancora poco investigate, nonostante l'importanza crescente di questi aspetti nell'ottica della sostenibilità delle infrastrutture digitali[432].

[431] J. MONSTADT, K. SALTZMAN, *How data centers have come to matter: Governing the spatial and environmental footprint of the 'digital gateway to Europe'*, in *International Journal of Urban and Regional Research*, 2025, 4, 757-758.
[432] P. WANG et al., *E-waste challenges of generative artificial intelligence*, in *Nature Computational Science*, 2024, 4(11), 818-823.

BIBLIOGRAFIA

- R. ABRAHAM, J. SCHNEIDER, J. VOM BROCKE, *Data governance: A conceptual framework, structured review, and research agenda*, in *International Journal of Information Management*, 2019, 49, 424-438.
- M. R. ALLEGRI, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in Rivista italiana di informatica e diritto, 2021, 3(2), 7-23.
- A. ALONGI, F. POMPEI, *Diritto della privacy e protezione dei dati personali – Il GDPR alla prova della data driven economy*, Roma, Tab Edizioni, 2021, 13-15.
- A. ALÙ, *La Governance di Internet oltre gli Stati? Gli inediti tratti del futuro ecosistema digitale*, in *Rivista italiana di informatica e diritto*, 2022, 4, 251-260.
- G. ALPA, *Il mercato unico digitale*, in *Contratto e impresa Europa*, 2021, 1, 1-3.
- G. ALPA, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. ZORZI GALGANO, Milano, Cedam - Wolters Kluwer, 2021, 11-32.
- A. ALPINI, *I vizi del consenso fra contratto e trattamento dei dati: la riconoscibilità dell'errore*, in *Persona e Mercato*, 2022, 205-215.
- M. AL-RUITHE, E. BENKHELIFA, K. HAMEED, *A systematic literature review of data governance and cloud data governance*, in *Personal and Ubiquitous Computing*, 2019, 23(5), 839-859.
- C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in *Law and Legal Institutions*, 2024, 11, 1-34.

- S. AMATO, *Appunti su aidos e privacy*, in *Teoria e Critica della regolazione sociale*, 2017, 1, 13-25.
- M. AMENDOLA, *Il principio solidaristico e il Data Governance Act*, Università di Salerno, 2023.
- D. AMRAM, G*overno dei dati, Open AI e salute: profili introduttivi*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2023, 2, 293-299.
- V. K. S. ANIL, A. B. BABATOPE, *The Role of Data Governance in Enhancing Cybersecurity Resilience for Global Enterprises*, in *World Journal of Advanced Research and Reviews*, 2024, 24(1), 1420-1432.
- H. ARENDT, *La vita della mente*, trad. it., Bologna, Il Mulino, 1987.
- H. ARENDT, *Vita activa. La condizione umana*, trad. it., Milano, Bompiani, 1964.
- J. ARNAL, *AI at Risk in the EU: It's Not Regulation, It's Implementation*, in *European Journal of Risk Regulation*, 2025, 1-10.
- J. ARPETTI, *Economia della privacy: una rassegna della letteratura*, in *Media Laws*, 2018, 2, 267-297.
- P. AURUCCI, F. DI TANO, *Dati personali e ricerca medica: condizioni, incoerenze e prospettive giuridiche a fronte dell'evoluzione interpretativa e applicativa del Garante per la protezione dei dati personali*, in *Biolaw Journal*, 2024, 3, 305-327.
- T. AVEN, *Risk assessment and risk management: Review of recent advances on their foundation*, in *European Journal of Operational Research*, 2016, 253(1), 1-13.
- E. BANI e E. MACCHIAVELLO, *Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati*, in *Financial Innovation tra disintermediazione e mercato*, a cura di V. FALCE, Torino, Giappichelli, 2015, 137-179.

- V. BARELA, *Accezione aggregata del dato: shuffle degli interessi in gioco e necessità di un approccio interdisciplinare a presidio del diritto di autodeterminazione della persona*, in *Diritto dell'Informazione e dell'Informatica*, 2, 2023, 159-187.
- J. P. BARLOW, *A Declaration of the Independence of Cyberspace*, 8 febbraio 1996, pubblicato online da Electronic Frontier Foundation
- R. BASILI, *Interoperabilità dei dati, metodologie di condivisione e prospettive: opportunità e rischi*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 33-64.
- M. BASSINI, *Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica*, in *Diritto Costituzionale*, 2023, 1, 83-112.
- F. BATTAGLIA, *La raccolta di dati da parte di Meta Platforms tra tutela dei dati personali, diritto della concorrenza e protezione dei consumatori*, in *Ordine internazionale e diritti umani*, 2022, 1048-1058.
- Z. BAUMAN, D. LYON, *Sesto potere. La sorveglianza nella modernità liquida*, Bari, Laterza, 2014.
- R. BECKER et al., *Secondary use of personal health data: when is it "further processing" under the GDPR, and what are the implications for data controllers?*, in *European Journal of Health Law*, 2022, 30(2), 129-157.
- L. BEDUSCHI, *La giurisprudenza di Strasburgo 2008-2010: gli altri diritti di libertà (artt. 8-11 CEDU)*, in *Dir. pen. cont.-Riv. trim.*, 2011, 1, 289-322.
- G. BELLOMO, *Contributo alla problematica della natura giuridica del "Data Protection Officer" (DPO)*, in *Consulta Online*, numero speciale *"Liber Amicorum per Pasquale Costanzo"*, 26 marzo 2020, 219-237.

- O. BENFELDT NIELSEN, *A Comprehensive Review of Data Governance Literature*, in *IRIS: Selected Papers of the Information Systems Research Seminar in Scandinavia*, 2017, 8(3), 120-133.
- B. BERISHA, E. MËZIU, *Big data analytics in cloud computing: an overview*, Seminar paper in the subject "Cloud Computing", University of Prishtina "Hasan Prishtina", 2021.
- F. BERTINI, *Artificial Intelligence and data privacy*, in *Sistemi intelligenti*, 2023, 35(2), 477-484.
- G. BIANCARDI, *Il trattamento dei dati personali nel prisma dell'ingiustificato arricchimento*, in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2024, 641-667.
- M. BIANCHINI, G. GASPARRI, G. RESTA et al., *Gli sviluppi tecnologici del diritto societario (Quaderno giuridico n. 23)*, Consob, maggio 2022.
- G. BINCOLETTO, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina: la tutela dei dati personali tra regole e prassi*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, Trento, Università degli Studi di Trento, 2024, 105-125.
- N. BOBBIO, *L'età dei diritti*, Torino, Einaudi, 1990.
- A.D. BLACK et al., *The Impact of eHealth on the Quality and Safety of Health Care: A Systematic Overview*, in *PLoS Medicine*, 2011, 8(1), 1-3.
- L. BOLOGNINI, *Valorizzazione economica dei dati personali e basi giuridiche*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024.
- A. BONFANTI, *La protezione dei dati personali nell'era digitale: considerazioni alla luce del quadro giuridico internazionale in*

materia di business e diritti umani, in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, 2017, 18(3), 477-497.

- F.Z. BORGESIUS et al., *The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects*, in *SCRIPTed*, 2023, 20, 352-381.
- M. BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato concorrenza regole*, 20(2), 2018, 223-245.
- O. BORGOGNO, M. SAVINI ZANGRANDI, *Data governance and the regulation of the platform economy*, in *Questioni di Economia e Finanza (Occasional Papers)*, Banca d'Italia, 2021.
- G. BORRIELLO, G. FRISTACHI, *Stato (d'assedio) digitale e strategia italiana di cybersicurezza*, in *Riv. Digit. Polit.*, 2022, 2(1–2), 157-178.
- B. BORRILLO, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, in *Dirittifondamentali.it*, 2020, 2, 326-356.
- A. BOURKA, P. DROGKARIS, *Security meets data protection: From risk management to systems engineering*, in *15 years of ENISA: A success story*, Publications Office of the European Union, 2019, 7-25.
- A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford-New York, Oxford University Press, 2020.
- F. BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Il diritto dell'informazione e dell'informatica*, 2023, 3, 481-518.
- F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, 199-256.

- P. BROUS, M. JANSSEN, R. VILMINKO-HEIKKINEN, *Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles*, in *5th International Conference on Electronic Government and the Information Systems Perspective (EGOV)*, Porto, Portugal, September 2016, 115-125.
- E. BRUGIOTTI, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Riv. on-line Dir. Fondam.*, 2013, 2, 9.
- J. BRUTHANS, *Connecting the Electronic Medical Records in the European Union – Where Do We Stand and Where Does It Go?*, in *Telehealth and Medicine Today*, 2024, 9(2), 1-2.
- B. BUZZELLI, *Dati sanitari e implementazione dell'Intelligenza Artificiale. Health data and implementation of Artificial Intelligence*, in *Intelligenza Artificiale e Sanità Digitale*, a cura di R. PICCOLO, Il Sileno Edizioni, 2024, 45-59.
- S. CACACE, *Autodeterminazione, paternalismo e responsabilità: l'uso primario dei dati sanitari nella relazione di cura e di fiducia fra medico e paziente*, in *Responsabilità Medica*, 2025, 3, 334-340.
- F. CAGGIA, *Cessione di dati personali per accedere al servizio digitale gratuito: il modello del "consenso rafforzato"*, in *I problemi dell'informazione nel diritto civile, oggi: studi in onore di Vincenzo Cuffaro*, a cura di M. D'AURIA, Roma Tre Press, 2022, 417-430.
- L. CALIFANO, *Come si governa la tecnologia digitale?*, in *Cultura giuridica e diritto vivente*, 2021, 1-11.
- F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Annali AISDUE*, 3, 2021, 58-75.

- E. CALZOLAIO, *Beni digitali e proprietà tra civil law e common law*, in *Rivista Critica del Diritto Privato*, Napoli, Jovene, 2023, 3, 287-326.
- E. CALZOLAIO, *Il regolamento sullo Spazio dei dati sanitari nella prospettiva della cittadinanza europea*, in *Diritto dell'Informazione e dell'Informatica*, 3, 2025, 315-335.
- S. CALZOLAIO, *Protezione dei dati personali, aggiornamento*, in *Digesto delle discipline pubblicistiche*, UTET, 2017.
- S. CALZOLAIO, *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in *Rivista Italiana di Informatica e Diritto*, 2024, 5(2), 13-33.
- C. CAMARDI, *Sulla Governance digitale europea: una proposta di confronto. European digital Governance: a call for discussion*, in *Accademia. Rivista dell'Associazione dei civilisti italiani – Confronti*, 2023, 1, 7-10.
- M. A. CAMILLERI, *Artificial intelligence governance: Ethical considerations and implications for social responsibility*, in *Expert Systems*, 2024, 41(7).
- F. CAMISA, A. SIMONCINI, *Il fattore umano e la regolazione della cybersecurity*, in *Mondo Digitale*, 2024, 1.
- S. CANALE, C. FABIANO, S. LEONARDI, *Il concetto di rischio e gli ambiti applicativi dell'analisi del rischio*, Istituto Strade Ferrovie Aeroporti, Quaderno n. 100, 1998.
- C. CARICATO, *Commento articolo 1*, in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 269-300.
- G. CARULLO, *Dati sanitari, sistemi sanitari nazionali e riuso dei dati*, in *Sanità rurale e assistenza sanitaria decentrata: Spagna e Italia. Esperienze a confronto = Sanidad rural y asistencia sanitaria*

descentralizada: España e Italia. Experiencia a debat, a cura di C. BOTTARI, P. J. TÁRRAGA LÓPEZ, J. CANTERO MARTÍNEZ, Napoli, Editoriale Scientifica, 2024, 401-420.

- G. CASCAVILLA, M. CONTI, *Cybersecurity: Uno stato dell'arte*, in *Formazione esperienziale: Proposte per la sicurezza digitale*, a cura di A. SURIAN, D. FRISON, Pensa MultiMedia, 2019, 13-18.
- F. CASCINI *et al.*, *Health data sharing: attitudes towards primary and secondary use of data. A systematic review,* in *EClinicalMedicine,* 2024, 2-4.
- R. CASO, *La società della mercificazione e della sorveglianza: dalla persona ai dati. Casi e problemi di diritto civile*, Milano, Ledizioni, 2021, 1-364.
- G. CERRINA FERONI, *Governare la rete per governare i diritti: quale cornice strutturale per il Data Governance Act?*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 23-32.
- M. CHAWKI, *Security and privacy in the era of electronic health records (EHRs)*, in *RAIS Journal for Social Sciences*, 2021, 5, 1.
- C. CHILIN, *Scambio di dati, conversione di formati e interoperabilità nella fornitura del servizio di intermediazione svolto dalle cooperative di dati*, in *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, a cura di F. BRAVO, Torino, Giappichelli, 2024, 785-800.
- F. CIMBALI, *La governance della sanità digitale,* 3, Wolters Kluwer Italia, 2023, 119-125.
- C. COLAPIETRO e A. MORETTI, *L'Intelligenza Artificiale nel dettato costituzionale: opportunità, incertezze e tutela dei dati personali*, in *BioLaw Journal-Rivista di BioDiritto*, 2020, (3), 359-387.

- V. COLCELLI, *Circolazione internazionale e trasferimento di campioni e dati personali: analisi di alcune caratteristiche del contratto,* in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, Trento, Università degli Studi di Trento, 2024, 127-146.
- V. COLOMBA, G. ZANETTI, *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in *Teoria e Critica della regolazione sociale*, 2017, 1, 27-39.
- G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, 5, 1193-1213.
- E. CREMONA, *Quando i dati diventano beni comuni: Modelli di data sharing e prospettive di riuso,* in *Rivista Italiana di Informatica e Diritto,* 2024, 5(2), 111-130.
- G. CRUPI, *Considerazioni preliminari sul riuso delle risorse digitali*, in *DigItalia*, 18(2), 2023, 15-23.
- V. CUFFARO, *Il diritto europeo sul trattamento dei dati e la sua applicazione in Italia: elementi per un bilancio ventennale*, in *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, Giappichelli, 2019, 3-17.
- V. CUFFARO, R. D'ORAZIO e V. RICCIUTO, *I dati personali nel diritto europeo: Un'analisi della disciplina introdotta dal Regolamento UE 2016/679*, Giappichelli, 2018.
- R. D'AGOSTINO, *La gestione dei dati nell'era digitale: un difficile bilanciamento fra esigenze di sicurezza, trasparenza e solidarietà*, in *P.A. Persona e Amministrazione*, 2024, 14(1), 555-578.
- L. DALLA CORTE, R. VAN BRAKEL, *Data protection impact assessment methods for the urban environment: A report for the Commissie Persoonsgegevens Amsterdam (CPA)*, Tilburg University, 2022, 2-4.

- A. DE CUPIS, *I diritti della personalità*, 2ª ed. riveduta e aggiornata, Milano, Giuffrè, 1926.
- G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy digitale*, a cura di E. TOSI, Milano, Giuffrè, 2019, 447-484.
- I. DE VIVO, *Sfide esistenziali e resilienze identitarie nella geopolitica informazionale: l'identikit europeo tra sovranità e costituzionalismo digitale*, in *Diritto pubblico europeo. Rassegna online*, 2024, 23(1), 168-189.
- A. DEL FORNO, *L'intelligenza artificiale nei processi gestori dell'impresa*, in *European Journal of Privacy Law & Technologies*, 2022, (2), 119-135.
- S. DEL GATTO, *La governance delle nuove tecnologie tra tentativi di regolazione e istanze di self regulation*. *Il caso del riconoscimento facciale*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2023, 1, 37-64.
- K. DEMETZOU, *Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2019, 35(6).
- K. DEMETZOU, *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, in *CEO Succession, Leadership, and (Dis)similarity*, in IFIP Advances in Information and Communication Technology, 2019, pp. 137-154.
- A. DEMMA, D. ROFFINELLA, *Dilemma del cyberspazio: privacy o condivisione?*, in *Rivista AEIT*, 2023, 110(2), 6-17.
- L. P. DIAMOND, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results (review)*, in *International Journal of Electronic Government Research*, 2005, 1(4), 63-67.

- F. DI CIOMMO, *Trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e Responsabilità*, 2002, 2, 121-134.
- A. DI CORINTO, *Data commons: privacy e cybersecurity sono diritti umani fondamentali*, in *Rivista italiana di informatica e diritto*, 2022, 4(1), 31-37.
- G. DI LORENZO E R. MESSINETTI, *Ordine giuridico ed evoluzione tecnologica, a proposito del recente libro su "i dati personali nel diritto europeo"*, in *NOMOS*, 2019, 3, 1-25.
- F. DI TANO, *Studi multicentrici, ruoli privacy e flussi di dati UE ed extra UE*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future: atti del convegno, Trento, 28 settembre 2023*, Trento, Università degli Studi di Trento, 2024, 39-56.
- G. DONNA, Modello di business, patrimonio strategico e creazione di valore, in Impresa Progetto, 2018, 2, 11-23.
- E. S. DOVE, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in *Journal of Law, Medicine & Ethics*, 2018, 46(4), 1013-1030.
- N. ELIAS, A. PERULLI E J. GOODWIN, *Verso una teoria delle comunità*, in *Cambio: rivista sulle trasformazioni sociali*, 2013, 6, 173-196.
- A. ENEGRÉN, *Il pensiero politico di Hannah Arendt*, Milano, FrancoAngeli, 1997, p. 60.
- P. ERTO, M. GIORGIO, I. IERVOLINO, *Probabilità e rischio*, in *Ambiente, rischio, comunicazione-Decidere nell'incertezza*, 2012, 4, 1-11
- F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, Giuffrè, 2019, 379.
- P. FALLETA e A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo*

sull'intelligenza artificiale e GDPR, in *Rivista italiana di informatica e diritto*, 2024, 6(1), 119-137.

- C. FARALLI, *Il diritto alla privacy. Profili storico-filosofici*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. ZORZI GALGANO, Milano, Cedam – Wolters Kluwer, 2019, 1-7.
- D. FÅHRÆUS, J. REICHEL, S. SLOKENBERGA, *The European Health Data Space: Challenges and Opportunities*, Stockholm, Sieps, 2024.
- M. FARINA, *Il diritto all'oblio nella governance dell'identificazione*, in *Federalismi.it*, 2020, 18, 95-111.
- M. FARINA, *Il cloud computing in ambito sanitario tra security e privacy*, Giuffrè Francis Lefebvre, 2019, 1-3.
- M. FEDERICO, B. PARENZO, *Le cooperative di dati tra persona e mercato: casi di studio*, in *De Iustitia*, 4, 2024, 1-12.
- F. FERRI, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in *Quaderni AISDUE*, 2024, 2, 1-20.
- G. FIORIGLIO, *La protezione dei dati sanitari nella società algoritmica. Profili informatico-giuridici*, in *Journal of Ethics and Legal Technologies*, 2021, 3(2), 79-102.
- G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di G. RESTA e V. ZENO-ZENCOVICH, Roma, Roma Tre Press, 2015, pp. 29-42.
- G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto dell'informazione e dell'informatica*, 2014, 29-42.
- R. FLOREANI, S. PETRUSSI, *Il GDPR in ambito assicurativo*, vol. 2, Giuffrè, 2025.

- G. FONSI, *Articolo 33 - Requisiti essenziali in materia di interoperabilità dei dati, dei meccanismi e servizi di condivisione dei dati nonché degli spazi comuni europei di dati*, in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2025, 681-696.
- T. E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Il Diritto dell'Informazione e dell'Informatica*, 2020, 3, 465-466.
- T. E. FROSINI, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, 2022, 51(1), 273-284.
- S. GATTI, *Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati*, in *European Data Law. European Journal of Privacy Law & Technologies*, 1, 2024, 158-177.
- R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, 34(2), 279-288.
- A. GENUS e A. STIRLING, *Collingridge and the dilemma of control: towards responsible and accountable innovation*, in *Research Policy*, 47(1), 2018, 61-69.
- G. GEORGIADIS, G. POELS, *Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review*, in *Computer Law & Security Review*, 2022, 44.
- A. GHIGLIA, *Commerciabilità dei dati personali: condizioni e limiti alla monetizzazione della nostra identità digitale nel contesto italiano ed europeo*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI Bologna, Il Mulino, 2024, 23-32.

- C. GILBERT, M.A. GILBERT, *Impact of General Data Protection Regulation (GDPR) on Data Breach Response Strategies (DBRS)*, in *International Journal of Research and Innovation in Social Science*, 2025, 9(14), 760-784.
- L. GIOS, *Strutturazione e gestione di una iniziativa di ricerca. Dallo sviluppo della documentazione alla gestione del dato*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, Trento, Università degli Studi di Trento, 2024, 21-38.
- S. GOBBATO, *Big data e "tutele convergenti" tra concorrenza, GDPR e Codice del consumo*, in *Media Laws*, 2019, 148-161.
- P. GUARDA e G. BINCOLETTO, *Diritto comparato della privacy e della protezione dei dati personali*, Ledizioni, 2023.
- G. GUERRA, *L'impatto dei dark patterns sul consenso dell'utente: la via europea per affrontare le nuove vulnerabilità*, in *Giustizia Civile.com*, 8, 2022, 1-48.
- M. GUGLIELMETTI, *Monetizzazione dei dati personali: breve analisi fondata sul valore della dignità umana e sulle «condizioni di mercato» della c.d. economia dei dati personali*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024, 33-53.
- W. HARTZOG e N. M. RICHARDS, *Privacy's constitutional moment and the limits of data protection*, in *Boston College Law Review*, 58(6), 2015, 1688-1761.
- W. HARTZOG e N. M. RICHARDS, *The surprising virtues of data loyalty*, in *71 Emory Law Journal*, 2022, 985-1033.
- W. HARTZOG, *Privacy's blueprint: The battle to control the design of new technologies*, Harvard University Press, 2018.

- M. HORÁK, V. STUPKA, M. HUSÁK, GDPR *Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform*, in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, 1-8.
- HORGAN, D., et al., *European Health Data Space - An Opportunity Now to Grasp the Future of Data-Driven Healthcare*, in *Healthcare (Basel)*, 2022, 10, 2-5.
- K.L. HUI e I. P. L. PNG, *The economics of privacy*, in T. HENDERSHOTT (ed.), *Handbooks in Information Systems: Volume 1: Economics and Information Systems*, Elsevier, 2006.
- A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi Parlamentari e di Politica Costituzionale*, 2021, (209), 31-52.
- M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari - Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Santarcangelo di Romagna, Maggioli Editore, 2025.
- A. IASELLI, M. IASELLI, *Nuove tecnologie, sicurezza e protezione dei dati*, Milano, Giuffrè Francis Lefebvre, 2024.
- M. IASELLI, *Guida alla nuova procedura di data breach*, Milano, Giuffrè Francis Lefebvre, 2021, 5-8.
- M. IPPOLITO, *Le cooperative di dati nella pubblica amministrazione italiana: alcune riflessioni in punto di valorizzazione dei dati alla luce del Data Governance Act e dell'AI Act*, in *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, a cura di F. BRAVO, Torino, Giappichelli, 2024, 545-576.
- LÉGIPRESSE, *Publication de l'AI Act : la CNIL émet des premiers éléments d'information et rappelle son rôle de promotion d'une IA respectueuse des droits des personnes sur leurs données*, in *Légipresse*, 2024, 401.

- N. IRTI, *Il tessitore di Goethe (per la decisione robotica)*, in *Decisione robotica*, a cura di A. CARLEO, Bologna, Il Mulino, 2019, 17-31.
- C. IURILLI, *La tutela del dato personale alla prova del Data Governance Act. Data sharing, reclamo e tutela giurisdizionale effettiva*, in *Judicium*, 3, Pacini Giuridica, 2024.
- S. R. JULAKANTI, N. S. K. SATTIRAJU, R. JULAKANTI, *Data Protection through Governance Frameworks*, in *Journal of Computational Analysis and Applications*, 2023, 31(1), 158-162.
- S. R. JULAKANTI, N. S. K. SATTIRAJU, R. JULAKANTI, *Security by Design: Integrating Governance into Data Systems*, in *International Journal of Communication Networks and Information Security (IJCNIS)*, 2022, 14(2), 393-399.
- D. KLOZA et al., *Towards a method for data protection impact assessment*, in *Policy Brief D. Pia. Lab*, 2020, 1, 1-2.
- O. KOKOULINA, *Challenges in Digital Compliance: Risk Assessment and Fundamental Rights under the GDPR and the EU AI Act*, in *CEUR Workshop Proceedings*, 2024.
- B.-J. KOOPS e R. E. LEENES, *Privacy regulation cannot be hardcoded: a critical comment on the "privacy by design" provision in data-protection law*, in *International Review of Law, Computers & Technology*, 28(2), 2014, 159-171.
- K. KOTSARELI, P. TSACHOURIDIS, *European Health Data Space: A New Era in EU Health*, in *HAPSc Policy Briefs Series*, 2023, 4, 2, 91-96.
- S. KYMPOUROPOULOS, *Real World Evidence: methodological issues and opportunities from the European Health Data Space*, in *BMC Medical Research Methodology*, 2023, 23, 185.
- F. LAGIOIA, G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi.it*, 2020, 11, 85-110.

- D. LANEY, *3D data management: Controlling data volume, velocity and variety*, META Group, 2001.
- S. M. LENER, *Personal data as counter-performance in exchange for contents or services after amendments to the Italian Consumer Code*, in *Rivista di Diritto Privato*, 1, 2024, 135-154.
- L.LESSIG, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.
- I. LIANOS, *Access to Health Data, Competition, and Regulatory Alternatives: Three Dimensions of Fairness*, in *Journal of Competition Law & Economics*, 2025, 44-46.
- C. LOBASCIO, *Droit et désinformation sanitaire: réponses juridiques et défis en Europe et en Italie*, in *Journal de droit de la santé et de l'assurance maladie*, 2025, 43.
- A. LO GIUDICE, *Quel diritto di essere lasciati soli*, in *Teoria e Critica della regolazione sociale*, 1, 2017, 7-10.
- A. LOMBARDI, *Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenze tra GDPR e AI Act | Data protection regulation and artificial intelligence regulation: relationships, similarities and differences between GDPR and AI Act*, in *European Journal of Privacy Law & Technologies*, 2023, (2), 240-252.
- P. LOMBARDI, *Sicurezza dei dati in ambito sanitario ed evoluzione tecnologica tra passato, presente e futuro*, in *Il Diritto dell'Economia*, 2021, 67, 106 (3), 49-82.
- R. K. LOMOTEY, S. KUMI, R. DETERS, *Data Trusts as a Service: Providing a platform for multi-party data sharing*, in *International Journal of Information Management Data Insights*, 2022, 2(1).
- F. LORÈ e P. MUSACCHIO, *Intelligenza Artificiale, tra profili di responsabilità e protezione dei dati personali: aspetti de jure condito e prospettive de jure condendo*, in *Amministrativ@mente-Rivista di*

ateneo dell'Università degli Studi di Roma "Foro Italico", 2024, 1, 27-70.

- F. LORÈ, *Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva?*, in *Amministrativ@ mente - Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2024, 65-90.
- Q. LU et al., *Responsible AI pattern catalogue: A collection of best practices for AI governance and engineering*, in *ACM Computing Surveys*, 2024, 56(7), 1-35.
- A. LUVISON, *La crittografia, uno snodo cruciale per la cybersicurezza*, in *Mondo Digitale*, 2016, 16.
- L. MAAß *et al.*, *Digital Public Health in Europe: Was the COVID-19 Pandemic an Enabler for Healthcare Digitalization?*, in *Digital Public Health - Interdisciplinary Perspectives*, a cura di H. ZEEB et al., Cham, Springer Nature Switzerland, 2024, 179-210.
- M. MAGGIOLINI, *Interoperabilità dei dati della pubblica amministrazione. Novità in materia di dati sanitari*, in *Amministrativ@mente - Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2025, (1), 386-401.
- A. MANTELERO, G. VACIAGO, *Reconciling data protection and cybersecurity: An operational approach for business sector*, in, *Privacy and data protection in software services*, a cura di R. SENIGAGLIA, C. IRTI, A. BERNES, Springer, 2022, 97-110.
- I. MARCOLONGO et al., *Internet governance: una questione di digital trust*, in *Rivista italiana di informatica e diritto*, 4(1), 2022, 241-250.
- J. S. MARCUS et al., *The European Health Data Space*, in *IPOL - Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament Policy Department Studies*, 2022.

- T. MARGONI, C. DUCUING, L. SCHIRRU, *Data Property, Data Governance and Common European Data Spaces*, in *Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht*, 2023.
- D. MARONGIU, *L'intelligenza artificiale "istituzionale": limiti (attuali) e potenzialità*, in *European Review of Digital Administration & Law*, 2020, 1, 37-53.
- P. MARSOCCI, *Sempre "al lavoro". Le garanzie costituzionali di persone e personalità connesse in Rete*, in *Rivista italiana di informatica e diritto*, 2021, 2, 73-88.
- Y. S. MARTÍN, A. KUNG, *Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering*, in *2018 IEEE European Symposium on Security and Privacy Workshops* (EuroS&PW), 2018, 108-111.
- Karlsruhe
- S. MARTINELLI, *I nuovi modelli per l'utilizzo dei dati: digital services e data economy*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024.
- N. MATTUCCI, *Mondo comune e responsabilità politica. Rileggendo la teoria politica di Hannah Arendt*, Macerata, EUM, 2008, 7-191.
- E. M. MENÉNDEZ SEBASTIÁN, *L'intelligenza artificiale nel settore pubblico: sulla perenne ricerca di un equilibrio tra efficienza e garanzie*, in *CERIDAP*, 2023, 2, 66-84.
- L. MERLA, *Big Data e diritto: una sfida all'effettività,* in *Media Laws*, 2021, 1, 218-233.
- A. A. MOLLO, *Prime riflessioni sul Regolamento Europeo sullo spazio europeo dei dati sanitari: l'uso secondario e il diritto di esclusione riguardo al trattamento dei dati sanitari elettronici personali*, in *BioLaw Journal - Rivista di BioDiritto*, 2025, 3, 11-29.

- J. MONSTADT, K. SALTZMAN, *How data centers have come to matter: Governing the spatial and environmental footprint of the 'digital gateway to Europe'*, in *International Journal of Urban and Regional Research*, 2025, 4, 757-758.
- A. G. MONTELEONE, *Il diritto alla portabilità dei dati: tra diritti della persona e diritti del mercato*, in *LUISS Law Review*, 2/2017, 202-213.
- V. MONTOZZI, *Le nuove sfide della regolazione dei dati: analisi di un modello a partire dall'intersezione tra protezione dei dati personali e concorrenza*, in *Rivista italiana di informatica e diritto*, 7, 2025, 501-524.
- A. MORACE PINELLI, *Introduzione*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 1-22.
- A. MORACE PINELLI, *Riflessioni introduttive,* in *Data Act: Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2025, 1-35.
- M. MORITZ, *Protection des données à caractère personnel et déploiement des IA: une conciliation impossible ? Le cas des décisions individuelles automatisées*, in *Dalloz IP/IT*, 2024, 506.
- P. MOURON, *Les conditions générales d'utilisation de Facebook sont soumises au Code de la consommation selon l'autorité de la concurrence italienne*, in *Revue européenne des médias et du numérique*, 49, 2019, 19-21.
- M. MURSIA e C. A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in *Media Laws*, 2, 2021, 165-189.

- F. NAFTALSKI e M. KERAMBRUN, *L'impact du « Data Act » sur les obligations des fournisseurs de services de traitement de données, en particulier sur les prestataires de services de cloud computing*, in *Dalloz IP/IT*, 2024, 211.
- A. F. NÄHER et al., *Secondary data for global health digitalisation*, in *The Lancet Digital Health*, 2023, 5(2), 93-101.
- J. NIELD, J. SCANLAN, E. ROEHRER, *Exploring consumer information-security awareness and preparedness of data-breach events,* in *Library Trends*, 2020, 68(4), 611-635.
- B. NIEUWESTEEG, M. FAURE, *An analysis of the effectiveness of the EU data breach notification obligation*, in *Computer Law & Security Review*, 2018, 34(6), 1232-1246.
- C. NOVELLI et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities,* in *European Journal of Risk Regulation*, 2025, 16(2), 566-590.
- A. ODDENINO, *Pervasività, centralità geopolitica e molteplicità delle istanze di tutela della cybersicurezza: elementi introduttivi*, in *Teoria e Critica della Regolazione Sociale/Theory and Criticism of Social Regulation*, 2024, 2(29), 15-24.
- R. OKORO, *Proposed data governance framework for small and medium scale enterprises (SMEs)*, in *Cornerstone: A Collection of Scholarly and Creative Works for Minnesota State University*, Master's thesis, Minnesota State University, Mankato, 2021.
- R. ORĂȘTEAN, R. SAVA, S. MĂRGINEAN, *Measuring healthcare digitalisation in the European Union: Trends and challenges*, in *Revista Economică*, 2022, 74(4), 64-74.
- S. ORLANDO, *Data vs capta: intorno alla definizione di dati*, in *Nuovo Diritto Civile*, 7(4), 2022, 14-53.
- S. ORLANDO, *Il coordinamento tra la direttiva 2019/770 e il GDPR. L'interessato consumatore,* in. *Persona e Mercato*, 2023, 222-241.

- S. ORLANDO, *La tutela penale della privacy nel cyberspazio,* in *Diritto penale contemporaneo - Rivista Trimestrale*, 2019, 2, 177-194.
- M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione,* in *Media Laws*, 2, 2018, 82-104.
- M. OROFINO, *One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in *Corti Supreme e Salute,* 2025, 1, 1-19.
- V. PAGNANELLI, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in *Rivista italiana di informatica e diritto*, 2021, 3(1), 11-26.
- H. J. PANDIT et al., *Towards a Semantic Specification for GDPR Data Breach Reporting,* in *Frontiers in Artificial Intelligence and Applications*, vol. 379, IOS Press, 131-136.
- A.G. PARISI. *Il regolamento generale sulla tutela dei dati personali. Responsabilità e sanzioni*, in *La nuova disciplina europea della privacy*, a cura di S. SICA, V. D'ANTONIO, G. M. RICCIO, Padova, CEDAM, 2016, 289-311.
- L. PASERI, *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, Torino, Giappichelli, 2025.
- L. PECCHIA, A. MACCARO, *Navigating European Healthcare Regulations Through a Historical Lens*, in *Digital Environments and Human Relations: Ethical Perspectives on AI Issues*, a cura di A. FABRIS, S. BELARDINELLI, Cham, Springer Nature Switzerland, 2024, 133-146.
- P. K. PEMMASANI, M. A. ABD NASARUDDIN, *Strengthening Public Sector Data Governance: Risk Management Strategies for*

Government Organizations, in *International Journal of Modern Computing*, 2022, 5(1), 108-118.

- A. C. PENEDO, *The Regulation of Data Spaces under the EU Data Strategy: Towards the "Act-ification" of the Fifth European Freedom for Data?*, in *European Journal of Law and Technology*, 2024, 15(1).
- V. S. Z. B. PEPOLI, *Profili di contrasto al cybercrime in iure condito e de iure condendo*, in *Rivista Italiana di Informatica e Diritto*, 4(2), 2022, 109-121.
- L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 39(3), 2023, 800-817.
- A. PIETROLETTI, A. NICOTRA, *Tutela della salute, sistemi digitali e privacy*, in *Rivista Italiana di Informatica e Diritto*, 2022, 4, 1, 283-294.
- G. PIGNATARO, *Circolazione dei dati tra modelli proprietari e contrattuali*, in *Media Laws*, 2, 2024, 1-26.
- G.A. PIMENTA RODRIGUES et al., *Understanding data breach from a global perspective: Incident visualization and data protection law review,* in *Data*, 2024, 9(2), 1-2.
- F. POLACCHINI, *Doveri costituzionali e principio di solidarietà*, Bologna, Bononia University Press, 2016.
- D. POLETTI, *Il quadro normativo del Data Governance Act: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 65-82.
- P. POLETTI, *Riforma dello spazio digitale europeo: DGA, proposta di Data Act e sicurezza delle informazioni*, in *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868.*

Commentario al «Data Governance Act», a cura di A. MORACE PINELLI, Pisa, Pacini Giuridica, 2024, 107-116.

- O. POLLICINO e M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield"*, a cura di G. RESTA e V. ZENO-ZENCOVICH, Roma, Roma Tre Press, 2016, 73-92.
- O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai Giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, a cura di G. RESTA, V. ZENO-ZENCOVICH, 2015, 7-28.
- B. PONTI, *Il rapporto tra cybersicurezza e tutela dei dati personali: sinergie, bilanciamenti e parallelismi*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 57-66.7
- G. PREITE, *L'habeas data sanitario come diritto all'autodeterminazione digitale del paziente*, in *Rivista elettronica di diritto, economia, management*, 2014, 105-116.
- N. PURTOVA, G. VAN MAANEN, *Data as an economic good, data as a commons, and data governance*, in *Law, Innovation and Technology*, 2023, 16(1), 1-42.
- F. RAGNO**,** *Il diritto fondamentale alla tutela dei dati personali e la dimensione transnazionale del private enforcement del GDPR*, in *Ordine internazionale e diritti umani*, 2020, 4, 818-838.
- É. RANÇON, *Publication du Data Act: Observations sous règlement (UE) 2023/2854 du Parlement et du Conseil du 13 décembre 2023*, in *Dalloz IP/IT*, 2024, 5.
- A. RANDAZZO, *Diritto all'identità personale e valori costituzionali. Le linee di un modello, traendo spunto da Luigi Pirandello*, in *Dirittifondamentali.it*, 2021, 3.

- J. R. REIDENBERG, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, in *Texas Law Review*, 1997, 76(3), 553-593.
- M. RENNA, *La disciplina del data breach nel GDPR: note su violazione dei dati personali e sicurezza del trattamento*, in *Actualidad jurídica iberoamericana*, 2023, 18, 992-1007.
- M. RESCIGNO, *L'impresa nell'era dell'intelligenza artificiale: un'evoluzione tranquilla o nulla sarà più lo stesso?*, Milano, Giuffrè Francis Lefebvre, 2023, 13-14.
- F. RESTA, *Cybersicurezza e protezione dati: un rapporto ambivalente*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 67-70.
- G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Il Diritto dell'Informazione e dell'Informatica*, 2015, 697-718.
- U. REVIGLIO, *The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview*, in *Internet Policy Review*, 11(3), 2022, 1-27.
- D. V. RICCIUTO, *Consenso al trattamento e contratto*, in *Persona e Mercato*, 2024, 13-26.
- N. M. RICHARDS e W. HARTZOG, *Taking trust seriously in privacy law*, in *Stanford Technology Law Review*, 19, 2017, 431-472.
- M. A. RIZZI, F. SERINI, *Una proposta di studio dei concetti di cybersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 115-136.
- S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 47.
- S. RODOTÀ, *La privacy tra individuo e collettività*, in *Politica del Diritto*, 1974, 5, 545.

- S. RODOTÀ, *Persona, libertà, tecnologia: Note per una discussione*, in *Diritto & Questioni Pubbliche*, 2005, 5, 25-29.
- S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Tecnologie e diritti*, Bologna, Il Mulino, 1995, 79-80.
- C.C. ROMITO, *Il GDPR nella micro, piccola e media impresa*, Milano, Giuffré, 2021, 131-132.
- J. ROY, *Polis and Oikos in Classical Athens*, in *Greece and Rome*, 1999, 46(1), 1-18.
- J. RUOHONEN, S. MICKELSSON, *Reflections on the Data Governance Act*, in *Digital Society*, 2(1), 2023, 10.
- M. RYAN, P. GÜRTLER, A. BOGUCKI, *Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces*, in *International Journal of Law and Information Technology*, 2024, 32, 20-21.
- C. SAILLANT, *Stratégie européenne pour les données : adoption du Data Act par le Conseil de l'Union européenne*, in *Dalloz actualité*, 2023.
- P. SAMMARCO, *Diritto digitale*, Giuffrè Francis Lefebvre, 2024, 1-4.
- M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, 2022, 4, 47-51.
- G. SARTORIS, *La tutela dei dati personali dei pazienti di fronte alle sfide della sanità digitale*, in *Diritto e Salute*, 2023, 33-46.
- C. SARRA, *Il diritto alla salute nell'era della datificazione*, in *Diritto alla salute, protezione dei dati personali e intelligenza artificiale*, a cura di C. SARRA, A. ZILIO, G. DE BONA, FrancoAngeli, Milano, 2025, 31-33.
- S. SCAGLIARINI, *Identità digitale e tutela della privacy, in Il diritto costituzionale e le sfide dell'innovazione tecnologica, atti del*

convegno, Genova, 18-19 giugno 2021, in *Quaderni del Gruppo di Pisa*, 2022.

- J. P. SCHNEIDER, J. ERNY, F. ENDERLEIN, *Collaborative Governance Structures for Interoperability in the EU's new data acts*, in *European Journal of Risk Regulation*, 2025, 16(1), 24-35.
- J. SCHUETT, *Risk management in the artificial intelligence act*, in *European Journal of Risk Regulation*, 2024, 15(2), 367-385.
- G. SDANGANELLI, *Il diritto all'oblio oncologico e i limiti all'uso dei dati sanitari nell'assicurazione digitale,* in *Federalismi.it*, 2025, 12, 230-252.
- D. J. SEIPP, *English judicial recognition of a right to privacy*, in *Oxford Journal of Legal Studies*, 1983, 3, 328.
- J. SÉNÉCHAL, *Vote des parlementaires européens sur l'AI Act : vers une réglementation accrue des IA, des modèles de fondation et des IA génératives, s'inspirant du DSA, du Data Act et du RGPD ?*, in *Dalloz actualité*, 2023.
- S. SICA, V., D'ANTONIO E G. M., RICCIO, *La nuova disciplina europea della privacy*, Wolters Kluwer, 2016.
- P. SILVA et al., *Privacy risk assessment and privacy-preserving data monitoring*, in *Expert Systems with Applications*, 2022, 200.
- A. SIMONCINI, *Do ut Data: quali limiti costituzionali alla cessione dei dati personali?*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024.
- S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI, *The European Health Data Space: Examining a New Era in Data Protection*, 1ª ed., Routledge, 2025.
- G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE Online*, 57(1), 2023, 339-369.

- A. SOLA, *Ambiti di interesse per la regolazione delle economie dei dati nel rapporto tra diritto e tecnologia*, in *Federalismi.it*, 10, 2023, 195-217.
- A. SOLA, *Economie dei dati, nuovi poteri ed autorità amministrative: il caso dell'Agenzia per la cybersicurezza nazionale*, in *Media Laws*, 2022, 3, 386-404.
- A. SOLA, *Primi cenni di regolazione europea nell'economia dei dati*, in *Media Laws*, 2021, 3, 188-209.
- D. J. SOLOVE, *Introduction: Privacy self-management and the consent dilemma*, in *Harvard Law Review*, 126(7), 2013, 1880-1903.
- S. SOMMARIVA *et al.*, *I registri in sanità e la creazione di conoscenza: dai database alla produzione scientifica*, in *Politiche Sanitarie*, 2015, 16(3), 168-176.
- A. SORRENTINO, A. F. SPAGNUOLO, *Cybersecurity e sovranità digitale nella protezione dei dati personali*, in *Rivista italiana di informatica e diritto*, 2024, 6(2), 685-701.
- C. SPINELLI, *Il regolamento (UE) 2022/868 sulla governance dei dati e le sue possibili ricadute sulle misure di inclusione lavorativa delle persone con disabilità*, in *Federalismi.it*, 2023, 9, 256-269.
- C. SPINIELLO, ScheDati. *Il diritto alla protezione dei dati personali nella legislazione europea*, in *Democrazia e Sicurezza*, 8(1), 2018, 143-188.
- S. STALLA-BOURDILLON, *Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU?*, in *European Journal of Risk Regulation*, 2025.
- P. STANZIONE, *Cybersicurezza e protezione dei dati personali*, in *Iura & Legal Systems*, 2025, 7(2), 76-84.
- P. STANZIONE, *Conclusioni*, in A. MORACE PINELLI, Dalla «Data Protection» alla «Data Governance»: il regolamento (UE)

2022/868. Commentario al «Data Governance Act», Pisa, Pacini Giuridica, 2024, 125-130.

- P. STANZIONE, *Introduzione,* in *Libertà e liceità del consenso nel trattamento dei dati personali*, a cura di S. ORLANDO, Firenze, Persona e Mercato ed., 2024, 5-7.
- I. STEPANOV, *Introducing a property right over data in the EU: the data producer's right - an evaluation,* in *International Review of Law, Computers & Technology*, 34(1), 2019, 65-86.
- J. TAMBA, *Interopérabilité des dossiers médicaux: ce qui change avec l'espace européen des données de santé*, in *Journal de droit de la santé et de l'assurance maladie*, 2025, 43, 131-138.
- M. TAMPIERI, *Cooperative di dati per la tutela della salute*, in *EU Data Cooperatives: L'ingresso delle cooperative di dati nell'ordinamento europeo*, a cura di F. BRAVO, Torino, Giappichelli, 2024, 434-442.
- S. THOBANI, *Il consenso nella regolazione della circolazione dei dati*, in *Persona e Mercato*, 2025, 2, 469-486.
- S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente,* in *Media Laws*, 2019, 131-147.
- S. THOBANI, *Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space),* in *Persona e Mercato*, 2024, 4, 1393-1399.
- M. TIMOTEO, *Alla ricerca di un diritto di proprietà dei dati. La via cinese,* in *Rivista Trimestrale di Diritto e Procedura Civile*, 2023, 4, 1157-1174.
- S. TIRIBELLI, *Oltre la privacy informazionale: libertà di scelta e di identità nell'era della profilazione algoritmica*, in *Itinerari*, LXI/2, 2022, 161-188.

- S. TORREGIANI, *Il Data Act: una versione europea del Data Nationalism?, Rivista italiana di informatica e diritto,* 2024, 5(2), 131-146.
- A. TORTORA, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del Data Protection Officer (DPO): incidenza sulla attività della pubblica amministrazione*, in *Amministrativ@mente - Rivista di ateneo dell'Università degli Studi di Roma "Foro Italico"*, 2018, 19-21.
- E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, Giuffrè, 2023.
- E. TOSI, *Dati personali e contratto: un ossimoro*, in *European Journal of Privacy Law & Technologies*, 2, 2023, 71-92.
- E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019.
- C. A. TROVATO, *Commercializzazione dei dati personali: limiti e condizioni*, in *Legal Tech, Big Data e contratti smart per professionisti e imprese*, a cura di S. MARTINELLI, C. ROSSI CHAUVENET, Wolters Kluwer, Milano, 2022, 199-217.
- C. A. TROVATO, *Everything has its price? Una riflessione sull'ammissibilità delle pratiche di commercializzazione dei dati personali*, in *Commerciabilità dei dati personali: Profili economici, giuridici, etici della monetizzazione*, a cura di G. CERRINA FERONI, Bologna, Il Mulino, 2024, 301.
- S. VAN DRUMPT et al., *Secondary use under the European Health Data Space: setting the scene and towards a research agenda on privacy-enhancing technologies*, in *Frontiers in Digital Health*, 2025, 7, 2-3.

- J. S. VANEGAS, *La violazione dei requisiti di sicurezza informatica di cui all'articolo 32 del GDPR*, in *Rivista Italiana di Informatica e Diritto*, 2020, 2(2), 5-14.
- F. VECCHIO, *L'ingloriosa fine della direttiva Data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in *Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna*, 2014, (4), 212-220.
- V. V. G. VESCIO DI MARTIRANO, *La governance dei dati personali e potere dispositivo dell'interessato*, Milano, Giuffrè, 2024.
- S. VILLANI, *Il sistema di vigilanza sull'applicazione dell'AI Act: ognun per sé?*, in *Quaderni AISDUE*, 2024, 2, 1-20.
- A. VOLPI, *Il Disastro come Mezzo*, in *Power and Democracy*, 2021, 2(2), 45-56.
- P. WANG et al., *E-waste challenges of generative artificial intelligence*, in *Nature Computational Science*, 2024, 4(11), 818-823.
- S. D. WARREN, L. D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, 4(5), 193.
- P. WEILL, J. W. ROSS, *IT Governance: How top performers manage IT decision rights for superior results*, Harvard Business School, Boston, 2004.
- P. A. WINN, *Older than the Bill of Rights: The Ancient Origins of the Right to Privacy*, 2010.
- H. ZECH, *Data as a tradeable commodity*, in A. DE FRANCESCHI (ed.), *European contract law and the digital single market: Implications of the digital revolution*, Cambridge, Intersentia, 2016, 51-80.
- V. ZENO-ZENCOVICH, *Big data e epistemologia giuridica, in Governance of/through Big Data*, a cura di G. RESTA, Roma, Roma Tre Press, 2023, 439-440.

- V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2018, 2, 1-7.
- A. ZILIO, *La disciplina del trattamento dei dati personali in ambito sanitario*, in *Diritto alla salute, protezione dei dati personali e intelligenza artificiale*, a cura di C. SARRA, A. ZILIO, G. DE BONA, FrancoAngeli, Milano, 2025, 81-85.
- S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.
- J.J. ZYGMUNTOWSKI, L. ZOBOLI, P.F. NEMITZ, *Embedding European values in data governance: a case for public data commons*, in *Internet Policy Review*, 2021, 10(3).

SITOGRAFIA

- A. BUONFRATE, S.E. BERRETTA e O. WOOD, *La rivoluzione digitale nel settore assicurativo: Big Tech, Big Data e Intelligenza Artificiale - Facciamo chiarezza*, https://www.costanzoeassociati.it/articoli-finanza-economia-diritto/la-rivoluzione-digitale-nel-settore-assicurativo-big-tech-big-data-e-intelligenza-artificiale-facciamo-chiarezza/, consultato da ultimo il 15.10.2025.
- CNIL, *Stratégie européenne pour la donnée : la CNIL et ses homologues se prononcent sur le Data Governance Act et le Data Act*, cnil.fr/sites/default/files/atoms/files/lettre_information_cnil_juillet_2022.html?, consultato da ultimo il 15.10.2025.
- Commissione Europea, *Entrata in vigore della legge su un'Europa interoperabile per migliorare la connessione dei servizi pubblici per i cittadini e le imprese*, 11 aprile 2024, https://ec.europa.eu/, consultato da ultimo il 22.10.2025.
- Commissione Europea, *New European Interoperability Framework: Promoting seamless services and data flows for European public administrations*, Publications Office of the European Union, 2017, https://europa.eu, consultato da ultimo il 22.10.2025.
- Commissione Europea, *Electronic cross-border health services*, *Health.Europa*, 8 agosto 2025, https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en, consultato da ultimo il 7.11.2025.
- Commissione Europea, *Regolamento sull'European Health Data Space (EHDS)*, https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en, consultato da ultimo il 7.11.2025.

- DAMA ITALY, *Sito ufficiale dell'associazione italiana per la Data Management Association International (DAMA)*, https://dama-italy.org/, consultato da ultimo il 24.10.2025.
- G. DELLA MORTE, *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, http://www.sidiblog.org/2020/03/30/la-tempesta-perfetta-covid-19-deroghe-alla-protezione-dei-dati-personali-ed-esigenze-di-sorveglianza-di-massa/, consultato da ultimo il 7.11.2025.
- GARANTE EUROPEO DELLA PROTEZIONE DEI DATI (GEPD), Sintesi del parere del GEPD del 7 marzo 2012 sul pacchetto di riforma della protezione dei dati, http://www.edps.europa.eu, consultato da ultimo il 14.10.2025.
- Y. N. HARARI, *Lessons from a year of Covid*, *Financial Times*, 8 luglio 2020, https://www.ft.com/content/f1b30f2c-84aa-4595-84f2-7816796d6841, consultato da ultimo il 7.11.2025.
- M. U. HAUK, C. PIERDONATI, *Ubiquità del mercato unico digitale*, 16 giugno 2025, Parlamento Europeo, https://www.europarl.europa.eu/factsheets/it/sheet/43/ubiquita-del-mercato-unico-digitale, consultato da ultimo il 22.10.2025.
- E. LETTA, *Much More Than a Market - Speed, Security, Solidarity: Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens* [Report], April 2024, Notre Europe/Institut Jacques Delors, https://institutdelors.eu/en/publications/much-more-than-a-market/, consultato da ultimo il 22.10.2025.
- S. MANCINI, I. MUMENI URBANI, M. PELLEGRINO, E. TRINCA, *Governance dei dati e dell'AI: una sinergia strategica per la PA*, in *Agenda Digitale 360*, 2 gennaio 2024, disponibile su: https://www.agendadigitale.eu, consultato da ultimo il 24.10.2025.

- SQS, *ISO 27701 - Sistema di Gestione per la Protezione dei Dati Personali*, disponibile online: https://www.sqs.it/iso27701.html, consultato il 13 novembre 2025.
- M. STEMPECK, *Sharing data is a form of corporate philanthropy*, in *Harvard Business Review*, 24 luglio 2014 https://hbr.org/2014/07/sharing-data-is-a-form-of-corporate-philanthropy, consultato da ultimo il 14.10.2025.
- U. VON DER LEYEN, *A Union That Strives for More: My Agenda for Europe (Political Guidelines for the Next European Commission 2019-2024)*, Commissione Europea, https://ec.europa.eu, consultato da ultimo il 22.10.2025.
- WORLD HEALTH ORGANIZATION (WHO), *WHO European Programme of Work 2020-2025 (EPW) - "United action for better health in Europe"*, World Health Organization, Regional Office for Europe, https://www.who.int/europe/news/item/13-09-2022-countries-in-the-european-region-adopt-first-ever-digital-health-action-plan, consultato da ultimo l'8.09.2025.

RIFERIMENTI NORMATIVI

- Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" (WP 248 rev. 01), Commissione Europea, 13 ottobre 2017.
- Commissione Europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni del 19 febbraio 2020, Una strategia europea per i dati, COM(2020) 66 final.
- Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, in Gazzetta ufficiale dell'Unione europea.
- Direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle telecomunicazioni, in Gazzetta ufficiale dell'Unione europea.
- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva sulla vita privata e le comunicazioni elettroniche), in Gazzetta ufficiale dell'Unione europea.
- Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico, in Gazzetta ufficiale dell'Unione europea.
- Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante 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 e che

modifica la direttiva 2002/58/CE, in Gazzetta ufficiale dell'Unione europea.
- Direttiva 2013/37/UE del Parlamento europeo e del Consiglio del 26 giugno 2013, che modifica la Direttiva 2003/98/CE, in Gazzetta ufficiale dell'Unione europea.
- Direttiva 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, GU L 119, 4.5.2016.
- Direttiva 2019/1024 del Parlamento Europeo e del Consiglio del 20 giugno 2019 relativa all'open data e alla riutilizzazione dell'informazione del settore pubblico (Direttiva sull'open data).
- EDPB, Linee guida 4/2019 sulla protezione dei dati fin dalla progettazione e per impostazione predefinita (adottate il 20 ottobre 2020, versione 2.0), 2021.
- EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Versione 2.1), 7 luglio 2021.
- EDPS Survey on Data Protection Impact Assessments under Article 39 of Regulation (EU) 2018/1725, 2020.
- EDPS, Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725, 2019.
- eHealth Network, Guidelines on the electronic exchange of health data under Cross-Border Directive 2011/24/EU: ePrescription and eDispensation of authorised medicinal products (Release 3.1), novembre 2024.

- eHealth Network, Guidelines on Patient Summary, Release 3.4. Guidelines on the electronic exchange of health data under Cross-Border Directive 2011/24/EU: Patient Summary, novembre 2024.
- ENISA, Handbook on Security of Personal Data Processing, 2017.
- ENISA, Online Platform for Security of Personal Data Processing: Reinforcing trust and security in the area of electronic communications and online services, December 2019.
- Garante per la protezione dei dati personali, Prescrizioni relative al trattamento dei dati genetici. Autorizzazione generale n. 8/2016.
- Gruppo di lavoro ex art. 29 sulla protezione dei dati personali (2018), *Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679*, Bruxelles: Commissione europea.
- 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 e alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati).
- Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018 relativo alla libera circolazione dei dati non personali nel mercato interno.
- Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo a un quadro europeo per la cibersicurezza (Cybersecurity Act).
- Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Data Governance Act).
- Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 3 ottobre 2023 relativo a un utilizzo equo e al ri-uso dei dati (Data Act).

- Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari (European Health Data Space - EHDS).
- Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 12 luglio 2024 che istituisce regole armonizzate sull'intelligenza artificiale (AI Act).

GIURISPRUDENZA

- Cass., 22 giugno 1985, n. 3769.
- CEDU, *Axel Springer c. Germania*, 7 febbraio 2012, ric. n. 39954/08.
- CEDU, *Huvig c. Francia*, 24 aprile 1990, ric. n. 11105/84.
- CEDU, *Malone c. Regno Unito*, 2 agosto 1984, ric. n. 8691/79;
- CEDU, *Von Hannover c. Germania*, 24 settembre 2004, ric. n. 59320/00.
- CGUE, causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, 13 maggio 2014.
- CGUE, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a.* e *Kärntner Landesregierung e a.*, 8 aprile 2014.
- CGUE, *Maximillian Schrems c. Data Protection Commissioner*, C-362/14, 6 ottobre 2015.
- Corte giust. (Grande Sezione), 1° ottobre 2019, causa C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:246.

ALLEGATI

Allegato 1

Annex 1

List of criteria for assessing whether processing operations are likely to result in high risks

In general, if two or more of the criteria in the list apply, the controller should carry out a DPIA. If the controller considers that in the specific case at hand, risks are not 'high' even though there is more than one 'yes', the controller has to explain and justify why they think the processing is in fact not 'high risk'. Each criterion is followed by some examples and counterexample on what would likely (not) trigger each criterion.

I Header	
Name of processing operation	[name]
Controller contact point	[function and contact details]
Record of processing operations	[record reference]
DPO consultation	[date of feedback]
Approval	[name and date]
II Criteria for processing "likely to result in **high risk**"	
Criterion	*Applicable? Yes [if so, describe how] / No [if borderline: why not?]*
1. Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting. *Examples: a bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions; profiling staff based on their transactions in a case management system with automatic reassignment of tasks.* *Counterexamples: standard appraisal interviews, voluntary 360° evaluations for helping staff to develop training plans.*	[Y (how?) / N]
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects Example: automated staff appraisal ("if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a "unsatisfactory" in your appraisal, no discussion"). *Counterexample: a news site showing articles in an order based on past visits of the user.*	[Y (how?) / N]
3. Systematic monitoring: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of staff internet use. *Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption, tracking movements via location data.* *Counterexample: open CCTV of garage entry not covering public space.*	[Y (how?) / N]

4. Sensitive data or data of a highly personal nature: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or data of highly personal nature. *Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification.* *Counterexample: photos are not sensitive as such (only when coupled with facial recognition / biometrics or used to infer other sensitive data).*	[Y (how?) / N]
5. Data processed on a large scale, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage: *Example: European databases on disease surveillance.* *Counterexample: invalidity procedures under Article 78 of the Staff Regulations in a medium-sized EUI .*	[Y (how?) / N]
6. Datasets matched or combined from different data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject. *Examples: cross-checking access control data and self-declared working hours following a suspicion of fraudulent declarations in an administrative inquiry (following the applicable rules).* *Counterexample: further use of data processed for a grant application when auditing the grant process.*	[Y (how?) / N]
7. Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified. *Examples: children, asylum seekers.* *Counterexamples: delegates in a Council Working Party (for attendance lists), members of expert groups (for travel cost reimbursement).*	[Y (how?) / N]
8. Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. *Examples: machine learning, connected cars, social media screening of job applicants.* *Counterexample: 1:1 biometric access control using fingerprints.*	[Y (how?) / N]
9. Preventing data subjects from exercising a right or using a service or a contract. *Examples: exclusion databases, credit screening.* *Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances).*	[Y (how?) / N]
III Conclusion	
Number of 'Yes' ticked above	[n]
Assessment: In general, if you tick two or more of the criteria in the list, you should carry out a DPIA. If you consider that in the specific case at hand, risks are not 'high' even though you have two or more 'yes', explain and justify why you think the processing is in fact not 'high risk'.	[explain]

Annex 2
Non-exhaustive list of some common processing operations and prima-facie indications of their risks

Positive list of processing operations prima facie requiring a DPIA (the numbers inside the brackets refer to the criteria in the template threshold assessment in Annex 1 such processing operations will likely trigger):

- Exclusion databases (2, 4, 9);
- large-scale processing of special categories of personal data (such as disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation) (1, 4, 5, 8);
- internet traffic analysis breaking encryption (data loss prevention tools) (1, 3, 8);
- e-recruitment tools automatically pre-selecting/excluding candidates without human intervention (1, 2, 8).

Allegato 3

Annex 3

Non-exhaustive list of some common processing operations not requiring a DPIA

Indicative list of processing operations prima facie not requiring a DPIA when carried out by Union institutions, bodies, offices and agencies acting as sole or joint controllers:

- Management of personal files under Article 26 of the Staff Regulations *as such*[6];
- Standard staff evaluation procedures under the Staff Regulations (annual appraisal);
- Standard 360° evaluations for helping staff members develop training plans;
- Standard staff selection procedures;
- Establishment of rights upon entry into service;
- Management of leave, flexitime and telework;
- Standard access control systems (non-biometric)[7];
- Standard CCTV on a limited scale (no facial recognition, coverage limited to entry/exit points, only on-premises, not in public space).