Studi di diritto dell'Unione europea
diretta da
A. Adinolfi, M. Condinanzi, P. Manzini, R. Mastroianni e F. Munari

Anna Fiorentini

Lo spazio europeo dei dati sanitari

Nuovi equilibri costituzionali tra mercato unico digitale e Unione europea della salute

Giappichelli

Studi di diritto dell'Unione europea

diretta da

A. Adinolfi, M. Condinanzi, P. Manzini, R. Mastroianni e F. Munari

3

La collana intende porsi come punto di riferimento per la pubblicazione di studi monografici, in particolare da parte di giovani studiosi, e di raccolte di saggi relativi al diritto dell'Unione europea, nei suoi aspetti istituzionali o di diritto materiale.

Le opere monografiche sono sottoposte ad una rigorosa procedura di referaggio secondo un procedimento concordato dai Direttori della collana con l'Editore.

IUSTITIAM COLIMUS

Anna Fiorentini

Lo spazio europeo dei dati sanitari

Nuovi equilibri costituzionali tra mercato unico digitale e Unione europea della salute

Giappichelli

© Copyright 2026 – G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-1949-7
ISBN/EAN 979-12-211-6803-7 (ebook - pdf)
ISBN/EAN 979-12-211-6804-4 (ebook - epub)

I volumi pubblicati nella presente Collana sono stati oggetto di procedura di doppio referaggio cieco (double blind peer review)*, secondo un procedimento standard concordato dai Direttori della collana con l'Editore, che ne conserva la relativa documentazione.*

This project has received funding from the European Union's under the ERASMUS-JMO-2023-HEI-TCH-RSCH Action Grant Budget-Based grant agreement No 101127551
Title: The protection of Health in Europe: Actors and Legal instruments
Acronym: HEAL
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by the European Union

HEAL JEAN MONNET MODULE

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

With the support of the Erasmus+ Programme of the European Union.

Opera distribuita con Licenza Creative Commons
Attribuzione – non commerciale – Non opere derivate 4.0 Internazionale

G. Giappichelli Editore

MARCHIO STORICO

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: Stampatre s.r.l. - Torino

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume/fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941, n. 633.

Le fotocopie effettuate per finalità di carattere professionale, economico o commerciale o comunque per uso diverso da quello personale possono essere effettuate a seguito di specifica autorizzazione rilasciata da CLEARedi, Centro Licenze e Autorizzazioni per le Riproduzioni Editoriali, Corso di Porta Romana 108, 20122 Milano, e-mail autorizzazioni@clearedi.org e sito web www.clearedi.org.

A Simone e Elia

Indice

pag.

Ringraziamenti XIII

Introduzione 1

1. Lo spazio europeo dei dati sanitari 1
   1.1. Il tassello mancante nel dibattito attuale 6
2. La metodologia di ricerca 8
3. La struttura dell'indagine 12

Parte I
Il fondamento costituzionale dello spazio europeo dei dati sanitari

Capitolo 1
La creazione di uno spazio europeo dei dati sanitari: obiettivi strategici e limiti costituzionali

1. Premessa 19
2. La progressiva erosione di spazi di competenza nazionale 30
   2.1. L'art. 114 TFUE: *longa manus* dell'Unione per intervenire in materia di sanità pubblica 30
   2.2. L'art. 16 TFUE: un ulteriore "grimaldello" per forzare le maglie del sistema di competenze 37
3. Una base giuridica "forte" per un'integrazione più profonda 45
   3.1. Gli obiettivi espliciti (e impliciti) dello spazio europeo dei dati sanitari 47
   3.2. Il ricorso agli artt. 114 e 16 TFUE per un quadro normativo armonizzato 53

pag.

4. La conformità dello spazio europeo dei dati sanitari rispetto al quadro costituzionale esistente 60
4.1. Il rispetto dell'autonomia degli Stati nella definizione delle loro politiche sanitarie 63
4.2. (*Segue*) Il sostegno degli *stakeholders* alle proposte della Commissione nel quadro delle consultazioni pubbliche 67
4.3. I limiti all'armonizzazione nel settore della sanità pubblica 69
4.4. (*Segue*) La voce flebile dei Parlamenti nazionali nell'ambito dei pareri del Protocollo n. 2 e del dialogo politico 75
5. Riflessioni conclusive 83

Capitolo 2
La dimensione economica e sociale dello spazio europeo dei dati sanitari: potenzialità e ostacoli alla sua realizzazione

1. Premessa 87
2. Lo spazio europeo dei dati sanitari come spazio di creazione di valore economico nel mercato unico digitale 90
2.1. I rapporti con i regolamenti della Strategia europea per i dati: DGA e DA 96
2.2. L'economia dei dati: accessibilità, circolazione e concorrenza 101
3. Lo spazio europeo dei dati sanitari come naturale sviluppo dello spazio europeo per la ricerca 105
3.1. Le prime esperienze in materia di ricerca scientifica tra collaborazione e integrazione 108
3.2. Il valore aggiunto dello spazio europeo dei dati sanitari 114
4. Lo spazio europeo dei dati sanitari come strumento di attuazione della Carta dei diritti fondamentali 118
4.1. Il diritto fondamentale alla salute 119
4.2. Il diritto fondamentale alla protezione dei dati personali 123
5. Gli ostacoli alla piena realizzazione della dimensione economica e sociale dello spazio europeo dei dati sanitari 128
5.1. L'uso primario dei dati sanitari 129
5.2. L'uso secondario dei dati sanitari 134
5.3. Il cuore della questione: quale bilanciamento tra i diritti e gli interessi in gioco? 138
6. Riflessioni conclusive 142

pag.

Parte II
Le tensioni (costituzionali e fisiologiche) tra lo spazio europeo dei dati sanitari e il GDPR

Capitolo 3
L'interpretazione del GDPR alla luce dello spazio europeo dei dati sanitari

1. Premessa 147
2. La tutela degli interessati al centro delle interpretazioni relative alla disciplina europea sui dati personali 152
   - 2.1. L'ambito di applicazione materiale 153
   - 2.2. I mezzi di conciliazione dei diritti e degli interessi in gioco 162
     - 2.2.1. Il diritto di accesso ai dati personali e le possibili limitazioni 163
     - 2.2.2. I dati sensibili e le deroghe al divieto generale di trattamento 169
3. Verso un equilibrio maggiormente in linea con gli obiettivi strategici del legislatore europeo 177
   - 3.1. Le scelte del legislatore nell'ambito dello spazio europeo dei dati sanitari 181
     - 3.1.1. La tutela dei diritti individuali (di controllo) 183
     - 3.1.2. I servizi e gli organismi per l'accesso ai dati sanitari elettronici 188
   - 3.2. I cambiamenti necessari nell'interpretazione del GDPR 194
     - 3.2.1. I limiti all'ambito di applicazione materiale 202
     - 3.2.2. Alcune ipotesi alternative di bilanciamento nell'interpretazione dei mezzi di conciliazione 210
4. Riflessioni conclusive 226

Capitolo 4
Il GDPR alla prova dello spazio europeo dei dati sanitari: nuovi scenari applicativi

1. Premessa 229
2. Gli ostacoli alla libera circolazione dei dati personali nel GDPR: Italia e Francia a confronto 235
   - 2.1. La frammentazione normativa 237
     - 2.1.1. Il Codice della privacy italiano e alcuni cenni (preliminari) al Fascicolo Sanitario Elettronico 241

pag.

2.1.2. La legge francese sulla protezione dei dati e il sistema centralizzato dell'*Health Data Hub* 248
2.1.3. L'imperfetta coincidenza tra le disposizioni nazionali e i possibili effetti sulla libera circolazione dei dati 251
2.2. La disomogeneità delle prassi amministrative 257
2.2.1. Il Garante per la protezione dei dati personali e la tutela della persona 258
2.2.2. La *Commission Nationale de l'Informatique et des Libertés* e le occasioni per la ricerca 261
2.2.3. Gli elementi di differenziazione tra le prassi amministrative delle autorità di controllo e i correttivi presenti nel GDPR 265
3. Verso un'applicazione del GDPR maggiormente uniforme alla luce delle novità introdotte dallo spazio europeo dei dati sanitari 269
3.1. Alcune ipotesi di revisione del testo del GDPR 276
3.1.1. Una definizione comune di "ricerca scientifica" 281
3.1.2. Le misure di garanzia e il margine di manovra degli Stati membri 284
3.2. La verifica della compatibilità del diritto nazionale di applicazione del GDPR con il diritto dell'Unione 291
3.2.1. (*Segue*) Nelle ipotesi di trattamento puramente "interne" 293
3.2.2. (*Segue*) Nelle ipotesi di trattamento a carattere transfrontaliero 299
4. Riflessioni conclusive 304

Conclusioni 307

Bibliografia 317

Ringraziamenti

Ho avuto l'opportunità di presentare e discutere le idee sviluppate in questo lavoro in diversi seminari organizzati presso l'Università di Trento, l'Università Bocconi di Milano, l'Università di Firenze, la *City University of London* e l'Università di Ghent. Sono profondamente grata a tutte le persone intervenute per le osservazioni e le critiche costruttive, e in particolare a Tamara Hervey, Mahsa Shabani e Diletta Danieli. Desidero inoltre ringraziare Markus Frischhut, David Townend, Elisabetta Biasin, Sofia Palmieri, Noemi Conditi, Daniele Sborlini, Giulia Bosi e Agnese Palazzi per gli stimoli e gli spunti di riflessione ricevuti in ulteriori occasioni di confronto.

Per la supervisione attenta e il sostegno costante lungo l'intero percorso che ha portato la tesi di dottorato in Diritto dell'Unione europea a trasformarsi in una monografia, e per aver creduto nel potenziale di un tema ancora poco esplorato e in continua evoluzione, desidero esprimere la mia più sincera gratitudine a Giacomo Di Federico. Sono inoltre riconoscente a Federico Casolari, Angela Carpi, Marco Inglese per i preziosi consigli e per le osservazioni formulate su una prima versione di questo scritto.

Ringrazio infine i Direttori della Collana per aver accolto questo lavoro, nonché la casa editrice Giappichelli, per la cura e la pazienza con cui ha accompagnato la nascita e la realizzazione di questo volume.

Introduzione

Sommario: 1. Lo spazio europeo dei dati sanitari. – 1.1. Il tassello mancante nel dibattito attuale. – 2. La metodologia di ricerca. – 3. La struttura dell'indagine.

1. Lo spazio europeo dei dati sanitari

Proposto nel maggio del 2022 [1], il regolamento sullo spazio europeo dei dati sanitari (*European Health Data Space* – EHDS) ha visto la luce all'alba del secondo mandato della Commissione von der Leyen [2]. L'iter legislativo di tale regolamento è stato piuttosto lineare e rapido, specialmente in seguito all'accelerazione impressa dalla presidenza belga per concludere i lavori prima dei cambiamenti istituzionali dovuti alle elezioni del Parlamento europeo di inizio giugno 2024. Tuttavia, il progresso del dossier sullo EHDS ha subito parziali rallentamenti per via della presenza di alcuni fattori legati, principalmente, al contesto storico-normativo in cui la proposta dello EHDS si colloca e alle sfide affrontate dal legislatore europeo nella formulazione delle norme.

In primo luogo, occorre ricordare l'intensa attività legislativa che, dal 2020, ha impegnato il legislatore europeo per la realizzazione di due ambiziosi progetti: lo sviluppo del mercato unico digitale tramite l'adozione dei regolamenti proposti nell'ambito della Strategia europea dei dati [3] e la creazione di

---

[1] Proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, COM(2022) 197 final, del 3 maggio 2022.

[2] Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

[3] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati, COM(2020) 66 final, del 19 febbraio 2020. Sull'attivismo del legislatore nel settore digitale, si rinvia, *ex multis*, all'analisi di C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO, *La trasformazione digitale in Europa. Diritti e principi*, Giappichelli, Torino, 2023, p. 3 ss. e O.

un'Unione europea della salute (UES) attraverso l'attuazione di un piano di riforme normative e istituzionali di ampia portata [4]. Sebbene lo EHDS costituisca un pilastro cruciale per l'attuazione di entrambi gli obiettivi menzionati, l'esigenza di raggiungere una sovranità digitale europea e di superare la situazione di crisi causata dalla pandemia da Covid-19, hanno orientato le priorità del legislatore verso l'adozione di altri regolamenti, tra cui quelli sulla governance dei dati (disciplina generale dello EHDS) [5], sui dati [6] e sull'Intelligenza Artificiale (IA) [7], nonché sul rafforzamento della governance sanitaria [8] e sulla gestione delle gravi minacce per la salute a carattere transfrontaliero [9].

In secondo luogo, è sufficiente menzionare la difficoltà di trovare un terreno comune di dialogo in seno al Parlamento europeo. Come sottolineato da uno dei correlatori del dossier sullo EHDS, l'europarlamentare ceco Tomislav Sokol, le maggiori divergenze di vedute sul testo sono emerse non tanto tra il Parlamento europeo e il Consiglio dell'Unione, quanto tra le diverse commissioni parlamentari coinvolte nella gestione del dossier [10]. In particolare, una

---

POLLICINO, *The Quadrangular Shape of the Geometry of Digital Power(s) and the Move Towards a Procedural Digital Constitutionalism*, in *Eur. Law J.*, 2023, vol. 29, nn. 1-2, p. 17 ss.

[4] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero, COM(2020) 724 final, dell'11 novembre 2020.

[5] 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 (DGA).

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

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

[8] Regolamento (UE) 2022/2370 del Parlamento europeo e del Consiglio del 23 novembre 2022 recante modifica del regolamento (CE) 851/2004, con il quale si crea un Centro europeo per la prevenzione e il controllo delle malattie; Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici; Decisione della Commissione del 16 settembre 2021 che istituisce l'autorità per la preparazione e la risposta alle emergenze sanitarie, C/2021/6712, final.

[9] Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio del 23 novembre 2022 relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE.

[10] In ragione del carattere trasversale delle questioni disciplinate dallo EHDS, la decisione della Conferenza dei presidenti di commissione del Parlamento europeo è stata quella di affiancare alla commissione LIBE la commissione ENVI, attribuendole una competenza

delle sfide principali è stata quella di conciliare l'approccio dei membri della commissione per le libertà civili, la giustizia e gli affari interni (LIBE), più rigoroso e restrittivo rispetto all'uso dei dati sanitari elettronici, e quello dei membri della commissione per l'ambiente, la sanità pubblica e la sicurezza alimentare (ENVI), maggiormente favorevole alle novità proposte dalla Commissione.

I primi hanno evidenziato i rischi derivanti dall'uso improprio dei dati sanitari, non solo in relazione alle possibili violazioni dei diritti alla privacy e alla protezione dei dati personali [11], ma anche rispetto agli effetti manipolativi sul comportamento delle persone, spesso all'origine di dinamiche discriminatorie e di stigmatizzazione [12]. All'opposto, i secondi hanno insistito sull'enorme potenziale dell'uso dei dati sanitari per ottimizzare la fornitura dei servizi e migliorare la programmazione in ambito sanitario, facilitare lo sviluppo di nuove terapie e farmaci, oltre che gestire, prevenire e rispondere a crisi sanitarie.

Tale sfida, per quanto centrale, non è stata la sola che il legislatore europeo ha dovuto affrontare nell'elaborazione del testo definitivo dello EHDS, che non si limita a disciplinare l'uso primario e secondario dei dati sanitari elettronici, ma regolamenta anche altri aspetti della sanità digitale. Si pensi, ad esempio, alle norme relative alle cartelle cliniche elettroniche e alle applicazioni per il benessere, la cui formulazione ha richiesto un eguale sforzo di bilanciamento per garantire la sicurezza di questi prodotti di sanità digitale e stimolare, al contempo, l'innovazione nel settore.

Alle questioni riguardanti il contemperamento dei diritti e degli interessi rilevanti nella regolamentazione di questa materia si è aggiunta la difficoltà di intervenire con un regolamento – e non più con una direttiva [13] – in un

condivisa (art. 58 regolamento del Parlamento europeo), e di prevedere la partecipazione della commissione per il mercato interno e la protezione dei consumatori (IMCO) e di quella per l'industria, la ricerca e l'energia (ITRE).

[11] Artt. 7 e 8 della Carta dei diritti fondamentali.

[12] Basti pensare all'uso di dati sanitari da parte dei datori di lavoro per decidere se assumere o meno una persona che presenta un elevato rischio di sviluppare una certa patologia, oppure da parte delle compagnie assicurative per fissare un premio maggiore sulla base di misurazioni ripetute della pressione arteriosa lungo un certo arco di tempo che fanno presumere che il soggetto in questione sia esposto maggiormente al rischio di attacchi cardiaci. Cfr. S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, in *Cal. Law Rev*., 2016, vol. 104, pp. 671-732; E.D. DE ARMOND, *To Cloack the Within: Protecting the Employees from Personality Testing*, in *DePaul Law Rev.*, 2012, vol. 61, pp. 1136-1137; K.B. BROTHERS, M.A. ROTHSTEIN, *Ethical, Legal and Social Implications of Incorporating Personalized Medicine into Healthcare*, in *Future Med.*, 2014, vol. 15, pp. 43-51; EDPS, *Opinion on the Communication from the Commission eHealth Action Plan 2012-2020-Innovative Healthcare for the 21st Century*, 2013, p. 6.

[13] Il riferimento è alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio del 9

ambito, quello della sanità pubblica [14], che rimane, almeno formalmente, in prevalenza di competenza nazionale. Inoltre, vale la pena di sottolineare che, con lo EHDS, il legislatore europeo si è cimentato nella realizzazione del primo – e, ad oggi, unico – esperimento normativo degli "spazi europei comuni di dati" [15], elaborando un modello regolatorio *ex novo* che, qualora si dimostri vincente, potrebbe essere replicato in altri settori.

Questi e ulteriori profili rendono lo studio dello EHDS di particolare interesse, tanto da essere oggetto di trattazione in diversi report elaborati recentemente da personalità di rilievo come Mario Draghi ed Enrico Letta per contribuire alla riflessione sul futuro dell'Unione [16]. Inoltre, sin dalle primissime fasi del processo legislativo, il suo testo ha suscitato un dibattito dottrinale molto vivace, coinvolgendo studiosi provenienti da diversi settori disciplinari (ad es. medicina, informatica ed economia) [17]. Concentrandosi sui contributi

---

marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera e, in particolare, l'art. 14 della stessa riguardante l'assistenza sanitaria online.

[14] Nel presente lavoro di ricerca, si è scelto di utilizzare l'espressione "sanità pubblica" e, in alcuni casi, "sanità digitale" per riferirsi a quelle misure adottate dall'Unione per tutelare la salute delle persone fisiche e della collettività nel suo complesso, anche attraverso l'uso di strumenti digitali. Tali espressioni sono quindi intese in senso ampio e assimilate al concetto di "salute umana" presente nei Trattati (v. art. 168 TFUE). Questa scelta è dettata dalla difficoltà, specialmente alla luce di atti come lo EHDS, di tracciare una netta distinzione tra obiettivi di sanità pubblica e quelli volti a garantire un adeguato livello di assistenza sanitaria per i singoli. Tuttavia, non si ignora l'esistenza di una differenza tra "sanità pubblica" e "assistenza sanitaria". Come spiegato efficacemente da Delhomme e Hervey: "*'Public health' has more of a collective dimension, whereas 'access to healthcare' has an individual connotation. 'Public health' can be understood as 'the management of health risks and the prevention of disease', whereas 'healthcare' refers to the 'provision of health services and medical care'*" (V. DELHOMME, T. HERVEY, *The European Union's Response to the Covid-19 Crisis and (the Legitimacy of) the Union's Legal Order*, in *Yearb. Eur. L.*, 2022, vol. 41, pp. 4-5). Sul punto si rinvia anche alle considerazioni svolte da A. DE RUIJTER, *EU Health Law & Policy: The Expansion of EU Power in Public Health and Health Care*, OUP, Oxford, 2019, pp. 62-63.

[15] Attualmente, infatti, dei quattordici spazi comuni europei di dati in fase di sviluppo, solamente quello in ambito sanitario ha portato all'elaborazione di un regolamento specifico. Cfr. https://digital-strategy.ec.europa.eu/it/policies/data-spaces.

[16] Cfr. M. DRAGHI, *The Future of European Competitiveness. Part B. In-Depth Analysis and Recommendations*, 2024, p. 200 e 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*, 2024, p. 81 in cui viene evidenziata l'importanza dello EHDS per massimizzare il potenziale dei dati, in particolare per promuovere la ricerca nel settore sanitario e per lo sviluppo del mercato interno.

[17] Si rinvia, *inter alia*, a S. RODRÍGUEZ-MEJÍAS et al., *Toward the European Health Data Space: The IMPaCT-Data Secure Infrastructure for EHR-Based Precision Medicine Research*, in *J. Biomed. Inform.*, 2024, vol. 156, pp. 1-6; R. RAAB et al., *Federated Electronic Health Records for the European Health Data Space*, in *Lancet Digit Health*, 2023, vol. 5, n. 11, pp. 840-847; D. HORGAN et al., *European Health Data Space – An Opportunity Now to Grasp the Future of Data-Driven Healthcare*, in *Healthcare*, 2022, vol. 10, n. 9, p. 1629.

dedicati all'analisi giuridica dello EHDS [18], è possibile osservare come l'attenzione sia stata catalizzata principalmente da quelle disposizioni che sollevano maggiori perplessità riguardo alla loro coerenza con le scelte operate dal legislatore europeo in altri atti di diritto derivato [19].

A questo proposito, un focus specifico è stato riservato alla relazione tra lo EHDS e il regolamento (UE) 2016/679 sulla protezione e libera circolazione dei dati personali (GDPR) [20], sollevando una molteplicità di rilievi critici, tra cui l'eccessiva ampiezza di alcune definizioni contenute nello EHDS, come quella relativa ai dati sanitari elettronici e alle finalità consentite per l'uso secondario degli stessi, nonché la scarsa chiarezza nel delineare il ruolo degli organismi responsabili per l'accesso ai dati sanitari e il rapporto tra le autorità di sanità digitale e le autorità di controllo previste dal GDPR. In linea generale, la maggior parte dei contributi dottrinali sembra assumere un orientamento critico rispetto allo EHDS, contestando in particolare la sua effettiva capacità di realizzare gli obiettivi prefissati [21], assicurando un adeguato bilanciamento tra il controllo delle persone fisiche sui loro dati e l'accesso agli stessi per finalità di interesse generale [22].

---

[18] Oltre agli autori citati in seguito, cfr. P. QUINN, E. ELLYNE, C. YAO, *Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?*, in *Comput. Law Secur. Rev*., 2024, vol. 54, pp. 1-15; S. GENOVESE, *The European Health Data Space: A Step towards Digital and Integrated Care Systems*, in *J. Integr. Care*, 2022, vol. 30, n. 4, pp. 363-372; R. VAN KESSEL et al., *The European Health Data Space Fails to Bridge Digital Divides*, in *BMJ*, 2022, p. 378; E. VAYENA, *Value from Health Data: European Opportunity to Catalyse Progress in Digital Health*, in *The Lancet*, 2021, p. 397; M. HENDOLIN, *Towards the European Health Data Space: From Diversity to a Common Framework*, in *Eurohealth*, 2021, vol. 27, p. 15; N. IACOB, F. SIMONELLI, *Towards a European Health Data Ecosystem*, in *Eur. J. Risk Reg*., 2020, vol. 11, p. 884.

[19] A. KISELEVA, P. DE HERT, *Creating a European Health Data Space. Obstacles in Four Key Legal Areas*, in *EPLR*, 2021, vol. 5, pp. 21-36.

[20] Su tali aspetti, si rinvia al parere congiunto 03/2022 di EDPB e EDPS sulla proposta di regolamento sullo spazio europeo dei dati sanitari commentato in dottrina, da G. BINCOLETTO, *The EDPB-EDPS Joint Opinion on the Commission Proposal for a Regulation on the European Health Data Space: Key Issues to be Considered in the Legislative Process*, in *Eur. Data Protection L. Rev.*, 2022, vol. 3, pp. 398-404 e da V. CIMINA, *The Proposal for a European Health Data Space: Between Pursued Objectives and Data Protection Challenges*, in *ERA Forum*, 2023, vol. 24, pp. 343-359.

[21] Tra gli altri, L. MARELLI et al., *The European Health Data Space: Too Big To Succeed?*, in *Health Policy*, 2023, p. 5 ss.

[22] Cfr. P. TERZIS, *Compromises and Asymmetries in the European Health Data Space*, in *EJHL*, 2023, vol. 30, pp. 345-363; M. SHABANI, S. YILMAZ, *Lawfulness in Secondary Use of Health Data. Interplay between Three Regulatory Frameworks of GDPR, DGA & EHDS*, in *TechReg*, 2022, pp. 128-134; S. SLOKENBERGA, *Scientific Research Regime 2.0? How the Proposed EHDS Regulation may Change the GDPR Research Regime*, in *TechReg*, 2022, pp. 135-147; D. SPAJIĆ, *Transforming the Secondary Use of Patient Data in the European Health Data*

1.1. Il tassello mancante nel dibattito attuale

In questo quadro, diversi sono gli aspetti dello EHDS che non sono ancora stati oggetto di una compiuta analisi dottrinale e che, invece, risultano meritevoli di essere indagati, specialmente dalla prospettiva dello studioso del diritto dell'Unione. Innanzitutto, nonostante venga riconosciuto l'effetto trasformativo della futura attuazione dello EHDS sull'organizzazione e sulla fornitura di assistenza sanitaria a livello nazionale [23], manca un contributo che affronti diffusamente i profili connessi alla legittimità di tale regolamento rispetto al quadro costituzionale europeo [24]. Inoltre, benché, come anticipato, non manchino analisi relative al rapporto tra lo EHDS e il GDPR, la dottrina si è concentrata principalmente su un aspetto: verificare che le norme dello EHDS siano rispettose del GDPR. Al contrario, non sembra esserci, al momento in cui si scrive, un'analisi che effettui l'operazione opposta, ossia che valuti se le norme del GDPR non debbano essere interpretate o attuate in modo differente alla luce delle novità introdotte dallo EHDS e, più in generale, dagli atti della Strategia europea per i dati.

Una simile prospettiva risulta giustificata poiché tali atti riflettono l'esigenza di massimizzare il valore dei dati, che si è cercato di soddisfare dapprima tramite la Strategia europea per i dati e, più recentemente, con il lancio della Strategia per la costruzione di un'Unione europea dei dati [25]. Questi sviluppi legislativi possono pertanto offrire spunti rilevanti per un'interpretazione evolutiva dell'assetto normativo vigente in materia di dati personali, interpretazione che si rivela oggi più che mai necessaria anche alla luce delle proposte di revisione del GDPR presentate dalla Commissione tra maggio e

---

Space: A Challenge for the Patient's Right to Medical Confidentiality?, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Routledge, London, 2025, pp. 87-109.

[23] L. MARELLI et al., *op. cit.*, 2023, p. 5: "*the EHDS will shape how healthcare delivery, and research and innovation activities across the EU are implemented. Its impact will be transformative*". Si veda anche, *inter alia*, F. KŘEPELKA, *Proposed Law for the European Health Data Space in Context*, in *Medicine, Law & Society*, 2023, vol. 16, n. 2, pp. 287-318 e T. PETROČNIK, *Health Data between Health(care) and the Data Economy*, in *TechReg*, 2022, p. 125.

[24] A conoscenza di chi scrive, l'unica eccezione è rappresentata da J. VAN DE GRONDEN, M. VEENBRINK, *EHDS and Free Movement of Patients: What EU Intervention is Needed?*, in *Eur. J. Health Law*, 2024, pp. 249-284.

[25] Questa Strategia è stata annunciata dalla Commissione nella comunicazione intitolata "Bussola per la competitività dell'UE", pubblicata nel gennaio 2025, a seguito dell'enfasi posta negli orientamenti politici per il mandato 2024-2029 sulla necessità di "*exploit the untapped potential of data*" (p. 10). Con tale Strategia, l'Unione intende "migliorare e agevolare la condivisione sicura di dati pubblici e privati, semplificare il regime normativo e la relativa applicazione e accelerare lo sviluppo di nuovi sistemi o applicazioni" (COM(2025) 30 final, p. 7).

novembre 2025 [26]. È fondamentale che tali proposte non siano il prodotto di contingenze o di pressioni esterne, ma che rappresentino invece l'esito di negoziazioni ponderate [27], capaci di preservare l'approccio valoriale che ha sinora guidato l'azione dell'Unione in questo settore.

Resta, in ogni caso, imprescindibile una riflessione più approfondita sul necessario coordinamento e sulla coerenza sistemica tra lo EHDS e il GDPR, al fine di evitare tensioni che possano compromettere la certezza del diritto e l'effettività delle tutele previste.

Nell'attuale dibattito dottrinale sorto attorno allo EHDS, dunque, non è presente un lavoro di ampio respiro [28] che, oltre a fornire una descrizione dettagliata del suo contenuto – per il quale non esistono ancora una giurisprudenza consolidata e prassi istituzionali –, affronti in modo strutturato alcune

---

[26] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2016/1036, (UE) 2016/1037, (UE) 2017/1129, (UE) 2023/1542 e (UE) 2024/573 per quanto riguarda l'estensione di alcune misure attenuanti disponibili per le piccole e medie imprese alle piccole imprese a media capitalizzazione e ulteriori misure di semplificazione, COM(2025)501 final, del 21 maggio 2025; proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 e delle 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 della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025.

[27] A tale riguardo, non appare lungimirante il ricorso alla tecnica legislativa dei "pacchetti" normativi. Come già evidenziato in dottrina, tale strumento, pur potendo favorire una maggiore coerenza sistemica tra atti eterogenei, rischia al contempo di generare effetti distorsivi sotto diversi profili: da un lato, può irrigidire indebitamente il processo decisionale, rendendo più difficile per le istituzioni dell'Unione raggiungere un accordo condiviso su singoli interventi normativi; dall'altro, comporta il pericolo che l'eventuale invalidità – anche parziale – di una componente del pacchetto finisca per compromettere la stabilità e la tenuta dell'intero complesso regolatorio. Cfr. P. DE PASQUALE, *Dalla flessibilità delle basi giuridiche alla normazione integrata: tecniche legislative funzionali alla rigidità del riparto di competenze nell'Unione*, in *DUE*, 2025, vol. 1, pp. 20-21. Per una critica più ampia allo strumento dei pacchetti, specialmente sotto il profilo della correttezza procedurale e del rischio di elusione delle garanzie istituzionali, si rinvia a: A. ALEMANNO, *The Legality of Omnibus Legislation Under EU Law: A Preliminary Analysis of Omnibus I Simplification Directive of CSRD and CSDD and its Legal Consequences on the EU Legal Order*, in *SSRN*, 2025; A. ALEMANNO, *The Omnibus Road to Constitutional Drift: How the Rise of Omnibus Legislation Undermines Procedural Integrity in the EU*, in *Verfassungsblog*, 2025.

[28] Fanno eccezione i lavori collettanei curati da S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025 e da N. DE GROVE VALDEYRON (sous la direction de), *Espace européen des données de santé et IA: enjeux juridiques et défis de mise en œuvre*, Presses de l'Université Toulouse Capitole, 2025, che offrono una panoramica dello EHDS attraverso contributi focalizzati su tematiche specifiche, quali i diritti degli individui nel nuovo contesto normativo, l'interazione con altri atti legislativi (come il DGA, il DA e l'AIA) e le implicazioni per i sistemi sanitari nazionali.

delle questioni di carattere sistematico e sostanziale che solleva lo EHDS. Per quanto riguarda le prime, ci si domanda se e in che misura tale regolamento si ponga in continuità o introduca invece elementi di novità rispetto all'avanzamento del processo di integrazione europea in ambito sanitario. Per quanto riguarda le questioni di carattere sostanziale, invece, si ritiene che le riflessioni svolte sul rapporto tra le norme dello EHDS e del GDPR dovrebbero essere ulteriormente sviluppate, interrogandosi sull'esistenza di tensioni tra i modelli regolatori adottati con questi due strumenti normativi.

Il presente lavoro si propone, senza pretese di esaustività, di colmare il vuoto dottrinale individuato, offrendo alcune risposte preliminari alle suddette questioni. L'obiettivo ultimo è quello di emancipare il dibattito su temi quali l'uso dei dati sanitari e delle cartelle cliniche elettroniche, spesso considerati estremamente tecnici e specialistici, da un esame quasi esclusivamente non giuridico [29]. Al contrario, queste tematiche sono di notevole interesse anche per gli studiosi del diritto, specialmente del diritto pubblico, il cui punto di vista può apportare un indubbio valore aggiunto per comprendere appieno le implicazioni giuridiche e costituzionali delle stesse. Ciò risulta ancor più evidente se consideriamo due aspetti: da un lato, l'impatto della digitalizzazione e della pandemia da Covid-19 sui delicati equilibri costituzionali nella tutela dei diritti fondamentali e nella relazione tra attori pubblici e privati; dall'altro, la risposta che tali trasformazioni hanno suscitato a livello sovranazionale, non più solo da parte della Corte di giustizia dell'Unione europea, ma anche da parte legislatore che, come anticipato, ha inaugurato un'intensa stagione di iniziative normative.

2. La metodologia di ricerca

Le questioni oggetto di trattazione in questo lavoro verranno affrontate adottando una metodologia di indagine composita, multi e interdisciplinare [30]. Questo approccio permette di combinare lo studio analitico del diritto primario

[29] A tale proposito, è d'obbligo precisare che, specialmente dai primi anni del XXI secolo, è emerso un crescente interesse, anche tra gli studiosi di diritto pubblico, per queste tematiche. In ambito digitale, dopo un primo periodo in cui l'attenzione era focalizzata prevalentemente sullo studio di profili come la governance di Internet, la responsabilità degli intermediari online, la proprietà intellettuale e la privacy, si è sviluppato un filone di ricerca che indaga le implicazioni costituzionali delle trasformazioni digitali. Similmente, lo studio del diritto sanitario, tradizionalmente riservato al diritto amministrativo nazionale, sta progressivamente acquisendo una propria dignità dottrinale nell'ambito del diritto internazionale.

[30] Per una descrizione di tali approcci metodologici, cfr. O. CORTEN, *Méthodologie du droit international public*, Éditions de l'Université de Bruxelles, Bruxelles, 2009, pp. 39-40.

e secondario dell'Unione, come interpretato dalla Corte di giustizia [31], con un'analisi dottrinale che integra contributi giuridici e provenienti da altri settori disciplinari (ad es. medico, informatico, etico ed economico) [32] al fine di migliorare la comprensione del testo normativo esaminato, valorizzando il contesto storico, politico e culturale in cui si colloca. La metodologia scelta consentirà inoltre di contestualizzare lo EHDS all'interno dell'ordinamento giuridico europeo secondo una duplice prospettiva: da un lato, come regolamento che permette di riflettere sulle traiettorie evolutive del processo di integrazione europea in ambito sanitario; dall'altro, come regolamento che consente di mettere in discussione gli equilibri costituzionali affermatisi in materia di protezione e libera circolazione dei dati personali.

Con riferimento alla prima prospettiva, il presente lavoro è debitore della teorizzazione del processo di integrazione europea offerta dalla teoria neofunzionalista, la quale viene qui utilizzata come supporto ricostruttivo della progressiva integrazione verificatasi nel campo della sanità pubblica [33]. A

---

[31] A livello di diritto derivato dell'Unione, la ricerca si concentrerà principalmente sui seguenti atti: il GDPR, la direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, il DGA, il DA e l'AIA. In aggiunta, oltre allo EHDS, verranno analizzati anche strumenti di *soft law*, come le comunicazioni e libri verdi della Commissione (v., in particolare, il capitolo 2), i quali, pur non avendo forza giuridica vincolante, possono comunque produrre effetti giuridici indiretti (cfr. L. SENDEN, *Soft Law in European Community Law*, Oxford Portland, Hart Publishing, 2004, p. 112), contribuendo, tra le altre cose, a chiarire le traiettorie evolutive che hanno caratterizzato e caratterizzano l'azione dell'Unione in ambiti specifici, come il mercato interno, la tutela della sanità pubblica e la ricerca.

[32] I principali scritti dottrinali analizzati sono quelli che hanno contribuito in modo significativo allo studio del diritto sanitario europeo e del diritto europeo per la protezione dei dati personali. In particolare, tra i primi, cfr. G. DI FEDERICO, S. NEGRI, *Unione europea e salute. Principi, azioni, diritti e standard qualitativi*, Cedam, Padova, 2019; A. DE RUIJTER, *EU Health Law & Policy: The Expansion of EU Power in Public Health and Health Care*, OUP, Oxford, 2019; T. HERVEY, J. MCHALE, *European Union Health Law: Themes and Implications. Law in Context*, CUP, Cambridge, 2015; F. COSTAMAGNA, *I servizi socio-sanitari nel mercato interno europeo*, Edizioni Scientifiche Italiane, Napoli, 2011. Tra i secondi, invece, cfr. O. LYNSKEY, *The Foundations of EU Data Protection Law*, OUP, Oxford, 2015; N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law Innov. Technol*, 2018; O. POLLICINO, *Judges, Privacy and Data Protection from a Multilevel Protection Perspective*, in *federalismi.it*, 2022; F. FERRI, *Il bilanciamento tra diritti fondamentali nel mercato unico digitale*, Giappichelli, Torino, 2022; P. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018. Per quanto riguarda, infine, le analisi non propriamente giuridiche, si rinvia ai riferimenti riportati alla nota 17.

[33] Sebbene il presente lavoro prenda in considerazione la prospettiva europea, è opportuno sottolineare come l'evoluzione descritta non possa essere pienamente compresa prescindendo dal più ampio quadro del diritto internazionale, nel quale si collocano obblighi e principi rilevanti – si pensi, in particolare, al Regolamento Sanitario Internazionale dell'Organizzazione

questo proposito, in particolare, verrà fatto riferimento agli effetti integrativi che sono stati recentemente individuati da autori come Brooks e al. [34], che a loro volta si sono ispirati al quadro teorico neo-funzionalista sviluppato da Haas e dai suoi allievi [35]. Inoltre, rifacendosi alle considerazioni dell'Avvocato generale Bot in *Brüstle*, verrà fatta propria la lettura del processo di integrazione che valorizza, accanto alla dimensione economica di tale processo, anche quella sociale [36]. Nella presente analisi, il termine "sociale" viene utilizzato in senso ampio. Il riferimento è infatti alla dimensione sociale dell'Unione che emerge dalle disposizioni dei Trattati relative ai valori e agli obiettivi (artt. 2 e 3 TUE), dalle clausole trasversali (artt. 8-13 TFUE), da alcuni obiettivi specifici (ad es. l'art. 168 TFUE), nonché dall'incorporazione della Carta tra le norme di diritto primario (art. 6, par. 1, TFUE) [37].

Quanto alla seconda prospettiva relativa agli equilibri costituzionali in materia di dati personali, la ricerca trae spunto dalle riflessioni che sono state sviluppate nell'ambito del filone dottrinale sul c.d. costituzionalismo digitale [38], valutando la capacità del diritto dell'Unione non tanto di limitare il potere degli attori pubblici e privati, quanto piuttosto di assicurare un equo bilanciamento tra diritti e interessi costituzionali nell'era digitale. È da queste premesse teoriche che prenderanno le mosse le considerazioni (*de lege lata* e

---

Mondiale della Sanità o alla protezione del diritto alla salute sancita in strumenti quali il Patto internazionale relativo ai diritti economici, sociali e culturali – che hanno contribuito a orientare tanto l'azione degli Stati quanto la cooperazione europea nel settore. Sulla tutela del diritto alla salute nel diritto internazionale, cfr. G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, p. 3 ss.; G.L. BURCI, B. TOEBES, *Research Handbook on Global Health Law*, Edward Elgar, Cheltenham, 2018; L.O. GOSTIN, *Global Health Law*, Harvard University Press, Cambridge, 2014.

[34] E. BROOKS et al., *EU Health Policy in the Aftermath of COVID-19: Neofunctionalism and Crisis-Driven Integration*, in *J. Eur. Public Policy*, 2023, vol. 30, n. 4, pp. 721-739.

[35] Cfr. E.B. HAAS, *The Uniting of Europe: Political, Social and Economic Forces*, 1950-1957, Stevens & Sons, London, 1958 e P.C. SCHMITTER, *Ernst B. Haas and the Legacy of Neofunctionalism*, in *J. Eur. Public Policy*, 2005, vol. 12, n. 2.

[36] Conclusioni dell'Avvocato generale Bot del 10 marzo 2011, causa C-34/10, *Brüstle c. Greenpeace*, ECLI:EU:C:2011:138.

[37] K. LÖRCHER, *Social Competences*, in N. BRUUN, K. LÖRCHER, I. SCHÖMANN (eds.), *The Lisbon Treaty and Social Europe*, Hart Publishing, Oxford, 2012, p. 165.

[38] G. PITRUZZELLA, *Il costituzionalismo digitale tra Stati Uniti e Europa*, in *Unione europea e diritti*, 2025, fasc. 2, pp. 1-11; E. CELESTE, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Routledge, London, 2023; G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, CUP, Cambridge, 2022; G. DE GREGORIO, *The Rise of Digital Constitutionalism in the European Union*, in *Int. J. Const. Law*, 2021, vol. 19, pp. 41-70; E. CELESTE, *Digital Constitutionalism: A New Systematic Theorisation*, in *Int. Rev. Law, Comput. Technol.*, 2019, vol. 33, n. 1, pp. 76-99; O. POLLICINO, *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism*, Hart, Oxford, 2021.

de lege ferenda) sulle scelte di bilanciamento nell'interpretazione e nell'applicazione del GDPR alla luce degli sviluppi normativi recenti in ambito digitale e, in particolare, dello EHDS.

Per fare ciò, oltre all'analisi della giurisprudenza della Corte sul GDPR, saranno esaminate, in chiave comparata [39], le normative nazionali di attuazione del GDPR in Italia e in Francia. La scelta di concentrare l'analisi su questi due ordinamenti risponde a una combinazione di ragioni che rendono il confronto particolarmente fecondo ai fini della presente indagine. In primo luogo, Italia e Francia appartengono a tradizioni giuridiche strutturalmente affini, contraddistinte da un'impostazione normativa e culturale che pone al centro la tutela dei diritti fondamentali della persona, tra cui la protezione dei dati personali. Questa impostazione garantista si distingue, almeno in parte, da quella prevalente in alcuni ordinamenti dell'Europa settentrionale, dove l'uso dei dati per finalità di interesse generale e ricerca scientifica è disciplinato in modo più permissivo, spesso prescindendo dal consenso dell'interessato, in un contesto istituzionale fondato sulla trasparenza.

In secondo luogo, sebbene l'attuazione del GDPR presenti differenze in tutti gli Stati membri, specialmente per quanto riguarda il trattamento dei dati sanitari a fini di ricerca scientifica (ad es. in relazione alla base giuridica o alle deroghe riconosciute ai diritti degli interessati), Italia e Francia si distinguono come gli unici due ordinamenti che, ai sensi dell'art. 9, par. 4, GDPR, subordinano tale trattamento al rispetto di condizioni specificamente definite dalle rispettive autorità di controllo: il Garante per la protezione dei dati personali (Garante) e la *Commission Nationale de l'Informatique et des Libertés* (CNIL). Altri Stati membri, invece, hanno optato per misure integrative differenti, quali l'individuazione delle categorie di soggetti autorizzati ad accedere ai dati, l'obbligo di sottoporre tali soggetti a vincoli di riservatezza, l'imposizione di finalità specifiche o requisiti di anonimizzazione oppure l'obbligo di ottenere il consenso in forma scritta [40].

Un ulteriore elemento che giustifica la comparazione risiede nel ruolo attivo che entrambe le autorità di controllo svolgono nell'attuazione del GDPR. Dalla seconda relazione della Commissione sull'applicazione del regolamento, il Garante e la CNIL figurano tra le autorità che hanno comminato il maggior numero di sanzioni pecuniarie, dopo quelle irlandesi e lussemburghesi [41].

---

[39] Cfr. G. WILSON, *Comparative Legal Scholarship*, in M. MCCONVILLE, H.C. WING (eds.), *Research Methods for Law*, Edinburgh University Press, Edinburgh, 2017, pp. 163-179.

[40] Commissione, *Report on the Implementation of Specific Provisions of the General Data Protection Regulation*, 2020, pp. 8-9.

[41] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati, COM(2024) 357 final, p. 8.

Tuttavia, in ambiti specifici come il trattamento dei dati per finalità di ricerca scientifica, le prassi delle due autorità divergono sensibilmente, sia per quanto riguarda l'interpretazione delle condizioni di liceità del trattamento sia nella valutazione delle garanzie richieste. Tali divergenze rendono i due ordinamenti emblematici per mettere in luce la frammentazione normativa ancora esistente nell'Unione in materia di dati personali.

Infine, la Francia rappresenta uno degli Stati membri più avanzati, sul piano normativo e infrastrutturale, nell'uso secondario dei dati sanitari, tanto da essere stata presa come modello di riferimento, insieme alla Finlandia, per la creazione dello EHDS. Al contrario, l'Italia, pur avendo avviato negli ultimi anni importanti riforme, continua a scontare difficoltà strutturali nella definizione di un quadro giuridico idoneo a conciliare efficacemente le esigenze di tutela e valorizzazione dei dati [42].

Quanto al profilo temporale, l'analisi fa riferimento all'assetto normativo vigente ad aprile 2026, nella consapevolezza che alcuni elementi potrebbero subire modifiche in seguito all'eventuale adozione del *Digital Omnibus*, presentato dalla Commissione il 19 novembre 2025. Tale proposta interviene infatti su diversi aspetti del GDPR e di altre normative rilevanti in materia digitale, tra cui il DGA, il DA e l'AIA. Di queste evoluzioni si darà comunque conto nel prosieguo, mettendo in evidenza gli aspetti ritenuti maggiormente rilevanti ai fini della presente ricerca che, come precisato, ha per oggetto principale lo EHDSR, il quale – allo stato attuale – non risulta essere stato oggetto di alcuna modifica da parte del legislatore europeo.

3. La struttura dell'indagine

Il volume presenta una struttura bipartita che riflette le linee di ricerca relative alle questioni sistematiche e sostanziali che lo EHDS pone (v. *supra*). Le due sezioni, in ogni caso, sono concepite come fasi consecutive di un percorso organico, che, pur concentrandosi su questioni che presentano ovviamente delle differenze sostanziali, al contempo offrono diversi punti di contatto. Alcuni dei temi e degli aspetti salienti emersi nei capitoli dedicati al "Fondamento costituzionale dello spazio europeo dei dati sanitari", come da titolo, costituiscono infatti una premessa necessaria alla sezione relativa alle "Tensioni (costituzionali e fisiologiche) tra lo spazio europeo dei dati sanitari e il GDPR".

---

[42] Per un approfondimento sul punto, cfr. capitolo 4, sezione 3.2.2 e A. FIORENTINI, *Vers la mise en œuvre de l'EEDS en Italie: les pièces manquantes du cadre réglementaire existant en matière de santé numérique*, in N. DE GROVE VALDEYRON, *op. cit*., 2025, pp. 115-130.

Nella prima parte, articolata in due capitoli, utilizzeremo l'analisi del fondamento costituzionale dello EHDS come osservatorio privilegiato per riflettere sull'evoluzione del processo di integrazione europea, concentrandoci, in particolare, su due dinamiche tipiche dello stesso: da un lato, l'utilizzo di basi giuridiche "forti" per intervenire in campi dove l'Unione dispone di una competenza limitata (capitolo 1) e, dall'altro, la continua aspirazione del legislatore europeo, soprattutto in tempi recenti, a raggiungere una sintesi tra obiettivi di carattere economico e sociale (capitolo 2).

Per quanto riguarda la prima dinamica, dopo una breve ricognizione delle principali tappe che hanno caratterizzato il processo di integrazione europea in materia di sanità pubblica, il capitolo 1 illustrerà come l'interpretazione estensiva fornita dalla Corte del campo di applicazione non più solo dell'art. 114 TFUE, ma anche dell'art. 16, par. 2, TFUE, consenta l'adozione di atti di diritto derivato, quali lo EHDS, che, pur trattando questioni che rientrano in ambiti (anche) di competenza nazionale, sono necessari per la realizzazione di obiettivi strategici dell'Unione (ad es. la creazione di un mercato unico digitale e di un'UES). Tali osservazioni consentiranno di mettere in luce gli aspetti problematici della scelta del legislatore di fondare lo EHDS su una base giuridica "forte" (artt. 114 e 16, par. 2, TFUE) per realizzare, secondo lo schema tipico della teoria neo-funzionalista, un'integrazione più profonda nel campo della sanità pubblica.

Passando poi alla seconda dinamica, nel capitolo 2 verrà analizzata la duplice dimensione economica e sociale dello EHDS, sottolineando come il raggiungimento degli obiettivi economici risulti funzionale alla realizzazione di quelli sociali. A tal fine, una volta illustrato il contributo dello EHDS alla creazione di valore economico nel mercato unico digitale, ci concentreremo sull'apporto di tale regolamento alla promozione della ricerca scientifica e all'attuazione dei diritti fondamentali della Carta. Infine, evidenzieremo gli ostacoli alla realizzazione di tali finalità, derivanti in particolare dall'assenza o dall'insufficiente coordinamento con altri atti di diritto derivato, e da come verrà operato il bilanciamento tra i diversi diritti e interessi potenzialmente contrastanti nell'interpretazione e applicazione dello EHDS.

Movendosi entro le coordinate costituzionali e normative individuate nella prima parte del lavoro, la seconda parte si concentrerà in modo più dettagliato sul rapporto tra lo EHDS e il GDPR. L'interrogativo di fondo sarà quello relativo alle scelte di bilanciamento necessarie a raggiungere un equilibrio ottimale tra la tutela del diritto del singolo al controllo sui dati personali e gli interessi di terzi e della collettività nel loro utilizzo, in modo da consentire la piena realizzazione degli obiettivi perseguiti dallo EHDS e dal GDPR. Lo scopo è verificare se tra questi due regolamenti sorgano delle

tensioni e, in tal caso, se sia possibile conciliarle tramite un ripensamento del modo in cui il GDPR è stato finora interpretato (capitolo 3) e applicato (capitolo 4).

In quest'ottica, nel capitolo 3, dopo aver illustrato i tratti essenziali dell'approccio interpretativo della Corte, si metterà in luce il contributo di quest'ultima alla concettualizzazione della disciplina sulla protezione dei dati personali come normativa votata essenzialmente alla tutela dei diritti (di controllo) degli interessati, sottolineandone le implicazioni per la tutela di altri interessi costituzionalmente rilevanti. Queste considerazioni permetteranno di mostrare l'inopportunità di utilizzare il medesimo approccio interpretativo anche per lo EHDS per evitare di pregiudicarne l'effettività, valutando piuttosto la possibilità di percorrere strade interpretative (almeno parzialmente) differenti alla luce dei recenti sviluppi normativi in materia di dati. Non potendo, per ovvie ragioni, procedere a un esame complessivo della giurisprudenza della Corte, l'analisi si limiterà a prendere in considerazione le pronunce relative alle disposizioni del GDPR sull'ambito di applicazione *ratione materiae* e su quelle che fungono da mezzi di conciliazione, ossia che consentono di bilanciare diritti e interessi potenzialmente confliggenti, poiché queste ultime hanno una rilevanza particolare anche per lo EHDS.

Infine, il capitolo 4 esaminerà gli ostacoli posti dall'applicazione eterogenea del GDPR da parte degli Stati membri, che compromettono il pieno perseguimento dell'obiettivo comune a entrambi i regolamenti considerati: la libera circolazione dei dati. A tale fine, saranno analizzate come casi studio la normativa italiana e quella francese, unitamente alle prassi amministrative delle rispettive autorità di controllo. Entrambi i sistemi giuridici presentano delle specificità che li rendono paradigmatici, offrendo, di conseguenza, preziosi spunti per comprendere meglio le contraddizioni insite nell'attuale assetto regolatorio. Una volta esaminate le principali differenze tra i due ordinamenti, si discuterà dell'opportunità di superare gli ostacoli derivanti dalla frammentazione normativa e dalla disomogeneità applicativa tra gli Stati membri attraverso una revisione del quadro normativo esistente in materia sia a livello sovranazionale che nazionale. Così come nel capitolo 3, anche in questo caso si è scelto di delimitare il campo d'indagine, circoscrivendolo all'esame delle norme nazionali di attuazione delle disposizioni del GDPR sul trattamento dei dati sanitari per finalità di ricerca. Questo perché tali disposizioni costituiscono uno degli esempi più emblematici di clausole di apertura facoltative, che attribuiscono agli Stati membri un ampio margine di discrezionalità nell'introdurre norme nazionali supplementari.

All'interno del perimetro appena tracciato, le pagine che seguono guideranno il lettore lungo un itinerario concepito per offrire alcune chiavi di lettura (tra le molteplici possibili) dello EHDS, che consentano di evidenziare i

profili istituzionali e materiali che caratterizzano tale regolamento. L'auspicio è che questo percorso contribuisca a far cogliere appieno la rilevanza dello EHDS, non solo nell'attuale quadro normativo sulla sanità digitale, ma anche nel più ampio processo che vede l'Unione europea assumere un ruolo sempre più centrale come attore fondamentale nella protezione della salute dei suoi cittadini.

Parte I
Il fondamento costituzionale dello spazio europeo dei dati sanitari

Capitolo 1
La creazione di uno spazio europeo dei dati sanitari: obiettivi strategici e limiti costituzionali

"*Is a Union of strictly limited powers always and by its very nature preferable to a Union capable of delivering more effective policy outcomes in the general interest? If we want the Union to manage some of our most difficult shared societal problems, are we willing to equip it with the necessary legal and policy tools? And if not, are we willing to accept that the price is either a less ambitious Union, or one that is prone to failure, in each case as a direct result of our own choices?*"

(Dougan, 2024) [1]

Sommario: 1. Premessa. – 2. La progressiva erosione di spazi di competenza nazionale. – 2.1. L'art. 114 TFUE: *longa manus* dell'Unione per intervenire in materia di sanità pubblica. – 2.2. L'art. 16 TFUE: un ulteriore "grimaldello" per forzare le maglie del sistema di competenze. – 3. Una base giuridica "forte" per un'integrazione più profonda. – 3.1. Gli obiettivi espliciti (e impliciti) dello spazio europeo dei dati sanitari. – 3.2. Il ricorso agli artt. 114 e 16 TFUE per un quadro normativo armonizzato. – 4. La conformità dello spazio europeo dei dati sanitari rispetto al quadro costituzionale esistente. – 4.1. Il rispetto dell'autonomia degli Stati nella definizione delle loro politiche sanitarie. – 4.2. (*Segue*) Il sostegno degli *stakeholders* alle proposte della Commissione nel quadro delle consultazioni pubbliche. – 4.3. I limiti all'armonizzazione nel settore della sanità pubblica. – 4.4. (*Segue*) La voce flebile dei Parlamenti nazionali nell'ambito dei pareri del Protocollo n. 2 e del dialogo politico. – 5. Riflessioni conclusive.

1. Premessa

Il fenomeno dell'integrazione europea è stato oggetto di diversi tentativi di teorizzazione. Tra le principali teorie che sono state sviluppate per spiegare le

[1] M. DOUGAN, *EU Competences in an Age of Complexity and Crisis: Challenges and Tensions in the System of Attributed Powers*, in *CMLRev.*, 2024, vol. 61, n. 1, p. 136.

dinamiche alla base di questo processo [2], quella funzionalista ha avuto maggiore fortuna rispetto alla teoria federalista e all'approccio intergovernativo [3]. In particolare, il fallimento del progetto di istituire uno Stato federale [4] ha contribuito all'affermarsi dell'idea secondo cui l'integrazione consiste in un processo graduale, in cui al progressivo svuotamento delle funzioni specifiche degli Stati si accompagna la contestuale attribuzione di poteri e competenze

---

[2] L. HOOGHE, G. MARKS, *Grand Theories of European Integration in the Twenty-First Century*, in *J. Eur. Public Policy*, 2019, vol. 26, n. 8, p. 1113.

[3] La versione classica della teoria federalista promuove la creazione di una struttura politica sovranazionale attraverso una scelta di tipo costituente e prevede il graduale trasferimento dei poteri dagli Stati a favore di un'entità federale. Questo per beneficiare degli effetti positivi di scala derivanti dall'unione delle economie europee e garantire la difesa attraverso un esercito comune (per maggiori approfondimenti sul punto, si rinvia a A. SPINELLI, E. ROSSI, *Il Manifesto di Ventotene*, Corriere della Sera, Milano, 2011, pp. 30-31: "Tutti gli uomini ragionevoli riconoscono ormai che non si può mantenere un equilibrio di stati europei indipendenti […] bisogna riconoscere che la Federazione Europea è l'unica concepibile garanzia che i rapporti con i popoli asiatici e americani si possono svolgere su una base di pacifica cooperazione, in attesa di un più lontano avvenire, in cui diventi possibile l'unità politica dell'intero globo". Cfr. P.S. GRAGLIA, *Altiero Spinelli*, Il Mulino, Bologna, 2010, p. 994 ss.; L. LACCHÈ, *Agli albori dell'Europa libera e unita. Per gli ottant'anni del Manifesto di Ventotene (1941-2021)*, in *Quaderni costituzionali*, 2021, vol. 4, p. 987 ss.; A. MANZELLA, *Il Manifesto della Costituzione*, in *Quaderni costituzionali*, 2021, vol. 4, p. 965 ss.). Al contrario, la teoria intergovernativa guarda al processo di integrazione europea dal punto di vista degli Stati, i quali puntano a stipulare accordi reciprocamente vantaggiosi. Sono i loro interessi, di natura prevalentemente economica, a orientare le scelte dei governi nazionali e non l'interesse sovranazionale (cfr. A. MORAVCSIK, *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*, UCL Press, London, 1999; S. HOFFMANN, *Obstinate or Obsolete? The Fate of the Nation-State and the Case of Western Europe*, in *Daedalus*, 1966, vol. 95, n. 3, pp. 862-915).

[4] Il progetto politico concernente l'affermarsi di una federazione europea subisce una forte battuta d'arresto con la mancata ratifica da parte della Francia del Trattato istitutivo della Comunità europea di difesa nel 1954. L'esigenza di individuare valori comuni sorge solo con il verificarsi di due momenti storici. Da un lato, la Conferenza intergovernativa che ha portato alla firma e alla successiva entrata in vigore del Trattato di Maastricht (1992-1993), il cui art. A sancisce che "[i]l presente trattato segna una nuova tappa nel processo di creazione di un'unione sempre più stretta tra i popoli dell'Europa, in cui le decisioni siano prese il più vicino possibile ai cittadini". Dall'altro, la convocazione, nel 2002, della Convenzione europea presieduta da Valéry Giscard d'Estaing e incaricata di redigere una Costituzione formale per l'Europa che, però, non venne mai alla luce per via della mancata ratifica da parte della Francia e dei Paesi Bassi (cfr. R. SCHÜTZE, *European Constitutional Law*, OUP, Oxford, 2021, pp. 17-37 e U. VILLANI, *Il cammino europeo tra crisi e sviluppi*, in *SIE*, 2023, vol. 1, pp. 9-10). Se in Francia il "disincanto" e "l'aperta ostilità per le politiche di Bruxelles" erano giustificate "dalla sensazione di un declino economico e sociale"; nei paesi più piccoli, come l'Olanda e le società scandinave, prevaleva invece il timore "della perdita di identità e dei vantaggi di un ordine sociale che era ormai parte di un modello di vita a cui sembrava impossibile rinunciare" (G. MAMMARELLA, *Storia d'Europa dal 1945 a oggi*, GLF Editori Laterza, Roma, 2006, p. 683).

all'ente sovranazionale [5]. Nel modello gradualistico di Monnet-Schuman [6], solo la realizzazione di obiettivi concreti, come l'integrazione in uno specifico settore economico, avrebbe portato alle condizioni necessarie per raggiungere i successivi livelli di integrazione sino ad arrivare a una federazione in grado di limitare la sovranità degli Stati in modo maggiore rispetto a quanto sarebbe successo a una qualsiasi altra organizzazione internazionale [7].

La teoria funzionalista ha conosciuto diverse varianti, tra cui quella neo-funzionalista [8], che ha contribuito ad ampliare la visione propria dei funzionalisti, introducendo il concetto di traboccamento (*spillover*) [9]. Nella prospettiva di una stretta correlazione tra diversi settori, i neo-funzionalisti ritengono che l'integrazione in ambito economico generi una dinamica espansiva volta all'interdipendenza di altri settori, come quello politico e sociale [10].

L'approccio teorico neo-funzionalista offre una spiegazione convincente del processo di progressivo ampliamento delle competenze europee nel settore

---

[5] R. SCHÜTZE, *From Dual to Cooperative Federalism: The Changing Structure of European Law*, OUP, Oxford, 2009, p. 70; E. CANNIZZARO, *Il diritto dell'integrazione europea. L'ordinamento dell'Unione*, Giappichelli, Torino, 2022, pp. 2-3.

[6] Sul contributo offerto da Jean Monnet al piano del ministro degli Affari esteri Robert Schuman e sull'esigenza di costruire un'Europa unita a partire dal mercato si veda anche G. MAMMARELLA, *Storia d'Europa dal 1945 a oggi*, GLF editori Laterza, Roma, 2006, p. 174 ss. e L. PATRUNO, *Il modello istituzionale europeo e l'idea di costituzione*, Giappichelli, Torino, 2006, p. 25 ss.

[7] Sin dalla celebre sentenza *van Gend en Loos*, è stato riconosciuto come "la Comunità costituisce un ordinamento giuridico di nuovo genere nel campo del diritto internazionale, a favore del quale gli Stati hanno rinunziato, anche se in settori limitati, ai loro poteri sovrani" (sentenza della Corte del 5 febbraio 1963, causa C-26/62, *van Gend en Loos*, ECLI:EU:C:1963:1, p. 23).

[8] E.B. HAAS, *The Uniting of Europe: Political, Social and Economic Forces*, 1950-1957, Stevens & Sons, London, 1958 e P.C. SCHMITTER, *Ernst B. Haas and the Legacy of Neofunctionalism*, in *J. Eur. Public Policy*, 2005, vol. 12, n. 2, pp. 255-272.

[9] C. BARNARD, *The Substantive Law of the EU. The Four Freedoms*, OUP, Oxford, 2019, pp. 19-20.

[10] Questo particolare effetto viene chiamato *spillover* funzionale e si differenzia da quello politico e coltivato. Il primo si verifica quando l'integrazione in un settore specifico porta a una maggiore consapevolezza e richiesta di integrazione da parte dei cittadini o dei leader politici. In altre parole, il successo iniziale di un'area può spingere gli attori pubblici o privati a cercare ulteriori livelli di integrazione in risposta alle aspettative pubbliche o alle nuove dinamiche politiche. Il secondo, invece, deriva da decisioni adottate da istituzioni sovranazionali e si verifica quando esse cercano attivamente di estendere l'integrazione da un settore a un altro, promuovendo un ampliamento dell'ambito di cooperazione. Ne consegue che, a differenza dello *spillover* funzionale, quelli politici e coltivati non sono automatici, bensì richiedono una volontà da parte degli attori pubblici/privati o delle istituzioni. Cfr. A. NIEMANN, *Neofunctionalism*, in M. RIDDERVOLD, J. TRONDAL, A. NEWSOME (eds.), *The Palgrave Handbook of EU Crises*, Springer International Publishing, Cham, 2021, pp. 115-133.

sanitario [11], che continua ad avanzare nonostante la resistenza degli Stati membri a cedere porzioni della propria sovranità [12]. Sin dalla bocciatura del progetto di costruire una Comunità sanitaria europea (*pool* bianco) da affiancare alla Comunità economica del carbone e dell'acciaio (*pool* nero) [13], gli Stati hanno infatti cercato di limitare l'intervento dell'Unione con riferimento a questioni legate alla dimensione sociale del mercato interno, come la sanità pubblica e la politica occupazionale, per preservare le prerogative nazionali [14]. Queste resistenze si sono tradotte in precise scelte di compromesso operate nell'elaborazione delle norme di diritto primario.

A tale proposito, è sufficiente ricordare che, fino al Trattato di Maastricht, la tutela della sanità pubblica è stata concepita quasi esclusivamente come eccezione invocabile dagli Stati membri per giustificare l'introduzione o il mantenimento di divieti o limitazioni alle libertà del mercato interno [15].

---

[11] Per un approfondimento sulla distinzione tra "*healthcare*" e "*public health*", cfr. V. DELHOMME, C. VAN OS, *Building the European Health Union (2019-2024): Successes, Limits and Future Perspectives*, in *EJRR*, 2025, vol. 16, n. 3, p. 3; V. DELHOMME, T. HERVEY, *The European Union's Response to the Covid-19 Crisis and (the Legitimacy of) the Union's Legal Order*, in *Yearb. Eur. L.*, 2022, vol. 41, p. 5; A. DE RUIJTER, *EU Health Law & Policy: The Expansion of EU Power in Public Health and Health Care*, OUP, Oxford, 2019, pp. 62-63.

[12] S.L. GREER, P. KURZER, *European Union Public Health Policy: Regional and Global Trends*, Routledge, London and New York, 2013; M. STEFFEN, *Health Governance in Europe: Issues, Challenges and Theories*, Routledge, London and New York, 2005.

[13] Sulla storia del progetto del c.d. *pool blanc*, presentato – forse troppo precocemente – dal ministro della salute francese Paul Ribeyre al Consiglio dei ministri francesi del 24 settembre 1952, cfr. A. DAVESBE, S. GUIGNER, *La Communauté européenne de la santé (1952-1954). Une redécouverte intergouvernementaliste du projet fonctionnaliste de "pool blanc"*, in *Politique européenne*, 2013, vol. 3, n. 41, p. 40-63. Si veda anche M. FRISCHHUT, *The Missing Keystone of the 'European Health Union'. Historic Development, Status Quo (De Lege Lata) and Ideas De Lege Ferenda*, in *ZaöRV*, 2025, vol. 85, p. 1015..

[14] S.L. GREER, *Uninvited Europeanization: Neofunctionalism and the EU in Health Policy*, in *J. Eur. Public Policy*, 2006, vol. 13, n. 1, p. 134.

[15] Artt. 36 e 59 del Trattato di Roma del 1957. Tra i casi in cui la Corte ha giudicato le limitazioni alle libertà fondamentali poste dal diritto nazionale come non giustificate da motivi di sanità pubblica, v. sentenze della Corte del 28 aprile 1998, causa C-158/96, *Kohll*, ECLI:EU:C:1998:171, punti 50-51; del 28 aprile 1998, causa C-120/95, *Decker*, ECLI:EU:C:1998:167, punti 41-45. Al contrario, tra i casi in cui la Corte ha ritenuto legittime le restrizioni alle libertà del mercato volte ad assicurare un elevato livello di salute, v. sentenze della Corte del 6 settembre 2012, causa C-544/10, *Deutsches Weintor*, ECLI:EU:C:2012:526, punto 53 e dell'1 giugno 2010, cause riunite C-570 e C-571/07, *Blanco Pérez*, ECLI:EU:C:2010:300, punto 65. Di recente, la Corte si è pronunciata anche sulle restrizioni alla libera circolazione dei cittadini poste al fine di limitare la diffusione del virus Covid-19. Nella causa *Nordic Info*, i giudici si sono espressi sulla compatibilità con il diritto dell'Unione (principi di proporzionalità e precauzione) della previsione e del mantenimento di restrizioni alle libertà del mercato quali misure di precauzione rispetto a una possibile "seconda ondata" della pandemia. In particolare, il Tribunale di primo grado di Bruxelles aveva effettuato un rinvio pregiudiziale alla Corte,

Successivamente, il fatto di attribuire alla salute una rilevanza autonoma nell'ordinamento europeo non ha determinato una cessione della materia a livello sovranazionale [16]. Così, nonostante alcune rilevanti modifiche introdotte dai Trattati di Amsterdam [17] e di Lisbona [18], la tutela della salute è

per chiedere se fossero compatibili con il diritto dell'Unione alcune misure adottate dal governo belga all'inizio del luglio 2020, tra cui il divieto di viaggi "non essenziali", ossia quelli verso e da specifici paesi considerati ad alto rischio di contagio, l'obbligo di quarantena e tamponi ai residenti in Belgio al loro ritorno da tali paesi, e i controlli effettuati alle frontiere belghe o nelle immediate vicinanze per garantire il rispetto delle restrizioni. Nella sua decisione, la Corte ha riconosciuto agli Stati membri la possibilità di adottare misure restrittive alle libertà del mercato a condizione che queste siano non discriminatorie e proporzionate (sentenza della Corte del 5 dicembre 2023, causa C-128/22, *Nordic Info BV*, ECLI:EU:C:2023:951, punto 98). Nell'effettuare il test di proporzionalità, i giudici hanno sottolineato come gli Stati membri possano prendere in considerazione le evidenze scientifiche di cui hanno conoscenza al momento in cui le misure sono state adottate. Allo stesso tempo, però, qualora tali evidenze non siano chiare, la Corte ha ammesso la possibilità di ricorrere al principio di precauzione (sentenza *Nordic Info BV*, punto 90). Per un commento sulla sentenza, cfr. M-L. ÖBERG, *The Legality of 'Covidfencing' Measures Under EU Free Movement Law:* Nordic Info BV v Belgische Staat, in *CMLRev*, 2025, vol. 62, pp. 1179-1204; *Editorial Comments Covid in the Case Law of the CJEU: Affirming EU Law Orthodoxy Even Under Extraordinary Circumstances*, in *CMLRev*., 2024, vol. 61, n. 3, p. 584 ss.; V. DELHOMME, *The Legality of Covid-19 Travel Restrictions in an 'Area without Internal Frontiers': Court of Justice (Grand Chamber) 5 December 2023, Case C-128/22, Nordic Info*, in *Eur. Const. Law Rev*., 2024, vol. 20, n. 2, pp. 307-328; D.F. POVSE, *So Long and See you in the Next Pandemic? The Court's One-and-Done Approach on Permissible Reasons to Restrict Freedom of Movement for Public Health Reasons in the Nordic Info case (C-128/22) of 5 December 2023*, in *European Law Blog*, 2023; P. CARBINI, *La Corte di giustizia si pronuncia sulla legittimità delle misure restrittive della libertà di circolazione durante il Covid-19*, in *Eurojus*, 2023. Per considerazioni di più ampia portata sulle giustificazioni che gli Stati membri possono invocare a sostegno della reintroduzione dei controlli alle frontiere, v. T. HERVEY, M. MICHALAK, *European Union Border Law During the COVID-19 Pandemic*, in *CMLRev*., 2025, vol. 62, p. 773.

[16] Art. 129 TCE.

[17] L'art. 152 TCE amplia la sfera di operatività della Comunità in vario modo. Ad esempio, menziona tra i settori di cooperazione tra gli Stati membri non solo le malattie e i grandi flagelli, ma anche tutte le fonti di pericolo per la salute umana e l'obiettivo del miglioramento della sanità pubblica (art. 152, par. 1, TCE). Viene attribuito al Consiglio il potere di adottare misure per la fissazione di parametri elevati di qualità e sicurezza degli organi e sostanze di origine umana, del sangue e degli emoderivati (art. 152, par. 4, lett. a), TCE), mentre le misure nei settori veterinario e fitosanitario finalizzate alla protezione della sanità pubblica possono essere adottate secondo la procedura della codecisione (art. 152, par. 4, lett. b), TCE).

[18] Rispetto all'art. 152 TCE, l'art. 168 TFUE introduce alcune modifiche che vanno nel senso di cedere maggiore autonomia decisionale alle istituzioni europee, riducendo il margine di manovra degli Stati membri. In particolare, l'Unione non è più obbligata a rispettare "appieno" le competenze nazionali in materia di organizzazione e fornitura di servizi sanitari e di assistenza medica (cfr. art. 168, par. 7, TFUE e art. 152, par. 5, TCE). Si ammette un'interferenza da parte dell'Unione nell'esercizio delle competenze degli Stati membri grazie all'attribuzione di un numero maggiore di poteri di supporto (cfr. art. 168, parr. 2 e 5, TFUE e art.

rimasta una competenza prevalentemente nazionale, rispetto alla quale l'Unione può svolgere un ruolo quasi esclusivamente di supporto, adottando misure di coordinamento o atti dotati di efficacia meramente esortativa [19].

I limiti formali posti dal quadro costituzionale, qui brevemente sintetizzati, non hanno tuttavia impedito all'Unione di intervenire in questo settore. Nel tempo, infatti, il legislatore europeo si è avvalso di diversi strumenti per influenzare (talvolta indebitamente) le competenze nazionali in ambito sanitario [20]. Ciò è avvenuto, ad esempio, attraverso l'uso della clausola sociale trasversale [21], l'introduzione dell'accesso alle cure sanitarie di qualità nel Pilastro

---

152, par. 2, TCE). L'Unione viene altresì dotata del potere di adottare atti con la procedura legislativa ordinaria per affrontare problemi comuni di sicurezza tramite, ad esempio, la fissazione di "parametri elevati di qualità e sicurezza dei medicinali e dei dispositivi di impiego medico" (art. 168, par. 4, lett. c), TFUE).

[19] L'art. 6, lett. a), TFUE attribuisce all'Unione la competenza di svolgere "azioni intese a sostenere, coordinare o completare l'azione degli Stati membri" con riguardo, *inter alia*, alla tutela e al miglioramento della salute umana. La natura complementare dell'azione dell'Unione impedisce l'adozione di atti giuridici vincolanti che comportino un'armonizzazione delle disposizioni legislative e regolamentari degli Stati membri (art. 2, par. 5, TFUE). Inoltre, ai sensi dell'art. 168, par. 7, TFUE, il legislatore europeo è obbligato a rispettare le responsabilità degli Stati nella definizione delle loro politiche sanitarie e nell'organizzazione e fornitura dei servizi sanitari nazionali. Ciò si evince anche dall'art. 35 della Carta in cui si afferma che il diritto di accesso alla protezione sanitaria e il diritto di ottenere cure mediche sono assicurati "alle condizioni stabilite dalle legislazioni e prassi nazionali".

[20] G. DI FEDERICO, *Principio di attribuzione e competenze esclusive degli Stati tra mito e realtà* (in corso di pubblicazione). L'A. individua sette modalità attraverso cui l'attività legislativa sovranazionale ha comportato una compressione delle prerogative degli Stati membri. Tra queste, ad esempio, viene menzionata l'adozione di un atto che si basa su una disposizione di diritto primario che consente l'armonizzazione, ma che, per obiettivo e/o contenuto, confligge con altre norme dei Trattati che, al contrario, escludono tale possibilità.

[21] Art. 9 TFUE. Sul tema, cfr. G. DI FEDERICO, S. NEGRI, *Unione europea e salute. Principi, azioni, diritti e sicurezza*, Cedam, Milano, 2019, p. 17 ss.; M.L. FLEAR, *Governing Public Health. EU Law, Health and Biopolitics*, Hart Publishing, Oxford, 2015, p. 54 ss.; T. HERVEY, J. MCHALE, *European Union Health Law: Themes and Implications. Law in Context*, CUP, Cambridge, 2015, p. 60 ss. Per quanto riguarda l'impatto dell'art. 9 TFUE sul riparto delle competenze, cfr. M.E. BARTOLONI, *The Horizontal Social Clause in a Legal Dimension*, in F. IPPOLITO, M.E. BARTOLONI, M. CONDINANZI, *The EU and the Proliferation of Integration Principles under the Lisbon Treaty*, Routledge, London, 2019, in cui viene sottolineato come le conseguenze derivanti dall'art. 9 TFUE sulla ripartizione delle competenze non sono da sottovalutare, specialmente se si considera che gli interessi protetti da tale disposizione rientrano in settori di competenza di supporto. Secondo l'A., l'art. 9 TFUE non dovrebbe essere interpretato come uno strumento volto ad ampliare i campi di applicazione delle competenze dell'Unione, bensì come strumento che, in linea con quanto disposto dall'art. 7 TFUE, consente di migliorare la coerenza tra le stesse (p. 83 ss.). Sulle clausole di integrazione, in generale, cfr. B. DE WITTE, *Integration Clauses – A Comparative Epilogue*, in F. IPPOLITO, M.E. BARTOLONI, M. CONDINANZI, *op. cit*., 2019, p. 181; J.H. JANS, *Stop the Integration Principle?*, in *Fordham Int'L.J.*, 2011, vol. 33, p. 1546.

europeo dei diritti sociali [22], il coordinamento economico delle politiche sanitarie nell'ambito del Semestre europeo [23] e soprattutto, per quanto qui rileva, mediante il ravvicinamento delle disposizioni legislative, regolamentari e amministrative nazionali che incidono sulla protezione della salute umana (v. *infra*). In questo processo, un ruolo determinante è stato giocato anche dai periodi di crisi [24]. Gli incidenti e le crisi sanitarie verificatesi in Europa hanno infatti aumentato la consapevolezza dell'importanza di un coordinamento

[22] Principio 16 del Pilastro europeo dei diritti sociali.

[23] Il Semestre europeo è uno strumento di governance economica che consente di coordinare le politiche economiche degli Stati membri, entro le quali rientrano a pieno titolo le scelte di politica sanitaria (raccomandazioni del Consiglio ECOFIN del 12 luglio 2016, sul funzionamento del semestre europeo nell'ambito dei diritti sociali, GUUE C 299/1 del 18 agosto 2016). Nel contesto del Semestre europeo, le prerogative nazionali vengono fortemente limitate in seno non solo alla Commissione, ma soprattutto al Consiglio che deve formulare le raccomandazioni finali, tra cui quelle relative agli investimenti strategici nel settore sanitario (ad es. digitalizzazione o tecnologie sanitarie). L'analisi del meccanismo del Semestre europeo, pensato per soddisfare esigenze di stabilità macroeconomica e non specificamente di tutela della salute, esula dallo scopo del presente capitolo. Tuttavia, per ulteriori approfondimenti, si rinvia a F. COSTAMAGNA, *Il coordinamento delle politiche economiche nell'ambito del Semestre europeo*, in O. PORCHIA (a cura di), *Governance economica europea. Strumenti dell'Unione, rapporto con l'ordinamento internazionale e ricadute nell'ordinamento interno*, Editoriale Scientifica, Napoli, 2015, p. 130; J. ZEITLIN, B. VANHERCKE, *Socializing the European Semester? Economic Governance and Social Policy Coordination in Europe 2020*, Sieps, Stockholm, 2014; B. VANHERCKE, *Europe 2020: Towards a More Social EU?*, in H. FRAZER et al. (eds.), *Europe 2020: Towards a More Social EU?*, Peter Lang, Bruxelles, 2010, pp. 15-44; T. CLEMENS, K. MICHELSEN, H. BRAND, *Supporting Health Systems in Europe: Added Value of EU Actions?*, in *Health Economics, Policy and Law*, 2014, vol. 9, n. 1, pp. 1-21; S.L. GREER, H. JARMAN, R. BAERTEN, *The New Political Economy of Health Care in the European Union: The Impact of Fiscal Governance*, in *Int. J. Health Serv*., 2016, vol. 46, n. 2, pp. 262-282; S. GIUDICI, *Il Semestre europeo alla prova del coordinamento delle politiche sanitarie degli Stati membri: evoluzione e prospettive alla luce del Next Generation EU*, in *SIE*, 2022, vol. 3, pp. 545-568.

[24] E. BROOKS, R. GEYER, *The Development of EU Health Policy and the Covid-19 Pandemic: Trends and Implications*, in *J. Eur. Integr*., 2020, vol. 42, n. 8, p. 1057. Per ulteriori riferimenti dottrinali sul ruolo delle crisi nell'avanzamento del processo di integrazione europea nel settore sanitario, cfr. V. DELHOMME, T. HERVEY, *op. cit*., 2022, p. 11; T. CLEMENS, H. BRAND, *Will COVID-19 Lead to a Major Change of the EU Public Health Mandate? A Renewed Approach to EU's Role Is Needed*, in *Eur. J. Public Health*, 2020, vol. 30, p. 624; S.L. GREER, A. DE RUIJTER, *EU Health Law and Policy in and After the COVID-19 Crisis*, in *Eur. J. Public Health*, 2020, vol. 30, p. 623; A. RENDA, R. CASTRO, *Towards Stronger EU Governance of Health Threats After the COVID-19 Pandemic*, in *Eur. J. Risk Regul*., 2020, vol. 11, p. 273. Uscendo dall'ambito sanitario, si rinvia invece a V. ANGHEL, E. JONES, *Is Europe Really Forged Through Crisis? Pandemic EU and the Russia-Ukraine War*, in *J. Eur. Public Policy*, 2023, vol. 30, n. 4, p. 766; F.M. FERRARA, H. KRIESI, *Crisis Pressures and European Integration*, in *J. Eur. Public Policy*, 2022, vol. 29, n. 9, p. 1351; A. BOIN, P. HART, A. MCCONNELL, *Crisis Exploitation: Political and Policy Impacts of Framing Contests*, in *J. Eur. Public Policy*, 2009, vol. 16, pp. 83-84.

sovranazionale efficace per affrontare i rischi transfrontalieri, portando alla formulazione di risposte specifiche [25]. Da ultimo, la pandemia da Covid-19 ha agito come catalizzatore di cambiamenti [26] sia a livello di diritto primario sia a livello di diritto derivato.

Rispetto al primo, sono state avanzate proposte, anche da parte dei cittadini europei [27], per modificare i Trattati al fine di prevedere, tra le altre cose, l'attribuzione all'Unione di una competenza concorrente in materia sanitaria [28].

---

[25] In questo senso, tra i principali atti di diritto derivato, possono essere ricordate le norme sulla valutazione e sulla commercializzazione dei medicinali (direttiva del Consiglio 65/65/CEE), sviluppate in risposta alla crisi della talidomide, e le norme sulla prevenzione di incidenti causati da determinate attività industriali (direttiva 82/501/CEE), elaborate in seguito alla crisi di diossina. Si pensi anche al regolamento sulla prevenzione e il controllo e l'eradicazione di alcune encefalopatie spongiformi trasmissibili (regolamento (CE) 999/2001) in risposta alla crisi della "mucca pazza", il regolamento che istituisce il Centro europeo per la prevenzione e il controllo delle malattie (regolamento (CE) 851/2004), adottato come conseguenza della crisi sanitaria SARS del 2003 e la decisione sulle gravi minacce per la salute a carattere transfrontaliero (decisione 1082/2013/UE), in risposta dell'influenza suina del 2009-2010. Cfr. V. DELHOMME, T. HERVEY, *op. cit*., 2022, p. 58.

[26] Cfr. T. CLEMENS, H. BRAND, *op. cit*., 2020, p. 624; S.L. GREER, A. DE RUIJTER, *op. cit*., 2020, p. 623; A. RENDA, R. CASTRO, *op. cit.*, 2020, p. 273; E. BROOKS, R. GEYER, *op. cit.*, 2020, p. 1057.

[27] I cittadini europei si sono espressi a favore di una revisione del diritto primario dell'Unione nell'ambito della Conferenza sul futuro dell'Europa (CoFoE), i cui lavori sono iniziati il 9 maggio 2021 in occasione della Festa dell'Europa, a seguito della firma della dichiarazione congiunta da parte del Presidente del Parlamento europeo David Sassoli, il Primo ministro portoghese António Costa a nome della presidenza del Consiglio e la Presidente della Commissione Ursula von der Leyen. Tra le raccomandazioni elaborate al termine della CoFoE figura quella di modificare i Trattati al fine di includere la tutela della salute umana tra le competenze concorrenti dell'Unione, sottraendola al novero di quelle di sostegno. Per un approfondimento sul tema e, in particolare, sulle differenti posizioni tenute dalle istituzioni europee circa il modo in cui dare seguito alle raccomandazioni dei cittadini dell'Unione, si consenta di rinviare a È. BULAND, A. FIORENTINI, *The Day After the CoFoE (Act II): The EU Treaty Revision at the Mercy of Enlargement?*, in *Quaderni AISDUE*, 2024, fasc. 1; A. FIORENTINI, *È.* BULAND, *The Day After the CoFoE: Is the EU Ready for a Revision of the Treaty*, in *Quaderni AISDUE*, 2022, pp. 295-300. Si vedano inoltre, *From Conference to Convention? Ideas and Prospects for a Reform of the EU Treaties*, in *CMLRev.*, 2022, vol. 59, pp. 1583-1596; F. RASPADORI, *La Conferenza sul futuro dell'Europa e le colonne d'Ercole della lontananza dei cittadini*, in *BlogDUE*, 2022, pp. 1-11; G. RIGGIO, *La parola ai cittadini: la Conferenza sul futuro dell'Europa*, in *Aggiornamenti sociali*, 2021, n. 5, p. 312 ss.; F. MARTINES, *La Conferenza sul futuro dell'Europa: uno strumento innovativo di partecipazione democratica per rafforzare la legittimità dell'Unione?,* in *Quaderni AISDUE*, 2021, vol. 3, pp. 9-29; B. NASCIMBENE, *L'iniziativa per una Conferenza sul futuro dell'Unione europea. Dalla "paura" all'"ambizione"*, in C. AMALFITANO, M. CONDINANZI, *Paura dell'Europa: spunti di razionalizzazione. Chi ha (ancora) paura dell'Europa?*, Giappichelli, Torino, 2020, p. 99 ss.; F. FABBRINI, *The Conference on the Future of Europe A New Model to Reform the EU?,* DCU Brexit Institute, Working Paper n. 12, 2019, pp. 1-19.

[28] Risoluzione del Parlamento europeo del 22 novembre 2023 sui progetti del Parlamento

Per quanto riguarda le disposizioni di diritto derivato, nel 2020 la Commissione ha presentato un pacchetto di iniziative volte a creare un'Unione europea della salute (UES) [29]. Al riguardo, alcuni autori, attingendo al quadro teorico neo-funzionalista, hanno evidenziato il verificarsi di tre effetti integrativi [30]: "*build-up*", "*spillover*" (funzionale) e "*spill-around*" [31].

---

europeo intesi a modificare i Trattati (2022/2051(INL)), p. 4. Nello specifico, il Parlamento europeo propone di modificare l'art. 4 TFUE in modo da annoverare tra le competenze concorrenti dell'Unione le questioni in materia di sanità pubblica, specialmente la tutela e il miglioramento della salute umana, con particolare riferimento alle minacce sanitarie transfrontaliere, inclusa la salute riproduttiva e l'approccio "One Health" (art. 4, par. 1, lett. e), TFUE). In aggiunta, vengono proposte diverse modifiche al testo dell'art. 168 TFUE, dalle quali si evince una maggiore consapevolezza circa l'importanza di adottare una visione olistica, capace di tenere insieme la salute delle persone, degli animali e dell'ambiente secondo il paradigma "One Health". Particolare attenzione è rivolta al quarto paragrafo dell'art. 168 TFUE, in cui viene aggiunto un riferimento esplicito alla possibilità di adottare misure: i) nel settore del benessere degli animali (lett. b); ii) che stabiliscano indicatori comuni sull'accesso universale e paritario a servizi sanitari di qualità e a prezzi accessibili, inclusa la salute riproduttiva (lett. c *bis*); iii) per monitorare e coordinare l'accesso a diagnosi, informazioni e terapie comuni per le malattie trasmissibili e non trasmissibili, comprese le malattie rare (lett. c *quater*); iv) per la notifica, il monitoraggio e la gestione tempestivi di gravi minacce per la salute a carattere transfrontaliero, in particolare in caso di pandemie (lett. c *ter*). Rispetto a queste ultime, si propone di concedere agli Stati membri la possibilità di mantenere o adottare misure di protezione rafforzate.

[29] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero, COM(2020) 724 final, dell'11 novembre 2020 e, più di recente, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, L'Unione europea della salute: agire insieme per la salute delle persone, COM(2024) 206 final, del 22 maggio 2024. Sebbene non si abbia una definizione giuridica di "Unione europea della salute", si ritiene più opportuno concepirla come politica settoriale dell'Unione, piuttosto che come un'entità giuridica autonoma. Ai fini della presente analisi, si adotta la definizione proposta da McKee e de Ruijter, secondo cui l'UES consiste in "*a series of initiatives developed by the European Union in response to the pandemic*" che "*will make an important contribution to protecting and promoting the health of Europe's citizens*" (M. McKee, A. de Ruijter, *The Path to a European Health Union*, in *The Lancet Regional Health – Europe*, 2024, vol. 36, p. 1). Sul punto, si veda anche V. Delhomme, C. van Os, *op. cit.*, 2025, pp. 13-19, V. Delhomme, T. Hervey, *op. cit.*, 2022, p. 58 e M. Frischhut, *op. cit*., p. 7. Per un'analisi dottrinale sull'UES come prossima tappa del processo di integrazione europea nel settore sanitario, v. M. Lazzaroni, *Le implicazioni istituzionali della pandemia da Covid-19: verso un'"Europa della salute"?*, in *SIE*, 2021, n. 2, pp. 391-414; A. Bucher, *Does Europe Need a Health Union?*, in *Policy Contribution*, 2022, n. 2, pp. 1-15; C. Seitz, *The European Health Union and the Protection of Public Health in the European Union: Is the European Union Prepared for Future Cross-Border Health Threats?*, in *ERA Forum*, 2022, vol. 23, pp. 561-566.

[30] E. Brooks et al., *EU Health Policy in the Aftermath of COVID-19: Neofunctionalism and Crisis-Driven Integration*, in *J. Eur. Public Policy*, 2023, vol. 30, n. 4, p. 727.

[31] Il termine "*spill-around*" si riferisce a un ampliamento del raggio d'azione dell'Unione

La maggior parte delle proposte relative alla creazione di un'UES presenta elementi di "*build up*", ossia di rafforzamento della governance sovranazionale, senza tuttavia modificare – almeno inizialmente – l'attuale assetto di competenze. Si pensi all'ampliamento dei poteri e del mandato dell'Agenzia europea per i medicinali (EMA) [32] e del Centro europeo per la prevenzione e il controllo (ECDC) [33], nonché alla creazione di un'unità della Commissione per le emergenze sanitarie, la preparazione e la risposta (HERA) [34]. Le restanti proposte, invece, rappresentano ipotesi di "*spillover*", ad esempio, nell'ambito dei finanziamenti europei per la gestione di minacce sanitarie e transfrontaliere (ad es. EU4Health [35] e rescEU [36]), oppure casi di "*spill-around*" in settori di coordinamento caratterizzati da una governance intergovernativa (ad es. il Consiglio per le crisi sanitarie) [37].

Una combinazione di tali elementi caratterizza anche il regolamento sullo spazio europeo dei dati sanitari (EHDS) [38], rendendolo un osservatorio privilegiato per riflettere sull'evoluzione del processo di integrazione europea nel campo della tutela alla salute. L'analisi del fondamento costituzionale dello EHDS permette di evidenziare come non sia più solo la competenza relativa al mercato interno (art. 114 TFUE), ma anche quella concernente la protezione e la libera circolazione dei dati personali (art. 16, par. 2, TFUE) a poter

---

che si realizza nel quadro di una governance intergovernativa. Cfr. E. BROOKS et al., *op. cit*., 2023, p. 272 ss.

[32] Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici.

[33] Regolamento (UE) 2022/2370 del Parlamento europeo e del Consiglio del 23 novembre 2022 recante modifica del regolamento (CE) 851/2004, con il quale si crea un Centro europeo per la prevenzione e il controllo delle malattie.

[34] Decisione della Commissione del 16 settembre 2021 che istituisce l'autorità per la preparazione e la risposta alle emergenze sanitarie, C/2021/6712, final.

[35] Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio del 24 marzo 2021 che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 ("programma UE per la salute") (EU4Health) e che abroga il regolamento (UE) 282/2014.

[36] Art. 12 decisione (UE) 2019/420 del Parlamento europeo e del Consiglio, del 13 marzo 2019, che modifica la decisione n. 1313/2013/UE su un meccanismo unionale di protezione civile.

[37] Art. 5 regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio del 23 novembre 2022 relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE.

[38] Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

generare il c.d. fenomeno della "*competence creep*" [39], che trova da sempre la sua massima espressione nel settore sanitario.

Nelle pagine successive, illustreremo come l'interpretazione estensiva del campo di applicazione degli artt. 114 e 16, par. 2 TFUE fornita dalla Corte di giustizia dell'Unione europea (Corte) rischi di legittimare l'adozione di atti di diritto derivato che, come lo EHDS, concorrono alla realizzazione di obiettivi strategici dell'Unione, pur trattando di questioni (anche) di competenza nazionale (sezione 2). In particolare, esamineremo come la scelta di fondare lo EHDS su una base giuridica "forte" [40], vale a dire sugli artt. 114 e

---

[39] S. GARBEN, *Competence Creep Revised*, in *J. Common Mark. Stud*., 2019, vol. 57, n. 2, p. 207 ss. descrive la "*competence creep*" non solo come l'effetto dell'adozione, a livello sovranazionale, di normative in settori che esulano dalle competenze attribuite all'Unione, ma anche come il risultato di altre forme di integrazione. Tra queste rientrano la legislazione indiretta o approccio trasversale, l'integrazione negativa attraverso la giurisprudenza, gli accordi internazionali, l'adozione di atti di *soft law*, i meccanismi di governance economica (ad es. Semestre europeo) e l'integrazione parallela che consiste nella conclusione di accordi intergovernativi soggetti al diritto internazionale (ad es. *Fiscal Compact*). Secondo l'A., tali forme di integrazione non possono essere giustificate dalla semplice interconnessione tra i settori di intervento. Il c.d. approccio di "*spillover*" o "*cross-cutting*", infatti, pur potendo garantire una governance efficace, solleva dubbi sulla legittimità democratica. In particolare, l'integrazione negativa appare più problematica rispetto alla legislazione indiretta, dal momento che priva i legislatori nazionali della possibilità di effettuare scelte politiche in aree di loro competenza. Secondo Garben, queste prassi sono "*highly non-transparent*" e comportano il trasferimento del potere decisionale politico dai legislatori nazionali ed europei ai giudici e all'esecutivo, "*leaving parliaments largely disempowered*" (p. 14). Pur riconoscendo l'importanza che l'ordinamento europeo conservi "*its necessary capacity for dynamism and adaptability*", come evidenziato anche da Weatherill (v. *infra*), Garben ritiene che una governance efficace "*must surely also be democratically legitimate*" (p. 15). Per queste ragioni, propone, da un lato, di limitare l'affermarsi della "*competence creep*", nelle sue varie declinazioni e, dall'altro, di accrescere le possibilità di ricorso alla legislazione europea, in particolare attraverso il metodo comunitario (p. 219). In senso analogo, si veda anche S. GARBEN, *From Sneaking to Striding: Combatting Competence Creep and Consolidating the EU Legislative Process*, in *Eur. Law J.*, 2020, vol. 26, nn. 5-6, p. 429 e G. DAVIES, *Democracy and Legitimacy in the Shadow of Purposive Competence*, in *Eur. Law J*., 2015, vol. 21, n. 1, p. 12 ss. Di segno opposto è invece la posizione di S. WEATHERILL, *Competence and Legitimacy*, in C. BARNARD, O. ODUDU (eds.), *The Outer Limits of European Union Law*, Hart, Portland, 2009, il quale evidenzia come la "*competence creep*" rappresenti il prezzo inevitabile della capacità delle istituzioni europee di individuare in modo flessibile soluzioni a problemi comuni (p. 27). Secondo Weatherill, il problema della "*competence creep*" non deve essere esagerato, poiché la "*flexibility in competence allocation promotes legitimacy in the sense of effective problem-solving*". Tuttavia, sottolinea l'importanza di evitare derive eccessive, suggerendo che una riforma istituzionale potrebbe costituire "*the most promising route to incubating a more critical culture in EU lawmaking*" (p. 34).

[40] Gli aggettivi "forte" e "debole" sono utilizzati per indicare quelle basi giuridiche che consentono all'Unione di intervenire in modo più incisivo (ad es. tramite armonizzazione) o meno nel disciplinare un certo settore.

16, par. 2, TFUE, possa produrre un effetto *spillover* nel campo della salute, dove i margini d'azione dell'Unione non sono particolarmente ampi (sezione 3). Tale effetto, se da un lato appare giustificato da esigenze di efficienza normativa, legate alla necessità di superare i limiti connessi all'applicazione della direttiva 2011/24/UE e del GDPR [41], dall'altro solleva interrogativi circa la conformità dello EHDS rispetto all'attuale riparto di competenze (sezione 4).

2. La progressiva erosione di spazi di competenza nazionale

In linea con le logiche di integrazione economica e sociopolitica di cui sopra, l'Unione europea ha progressivamente ampliato la propria sfera di influenza, occupandosi (più o meno legittimamente) di settori tradizionalmente di competenza degli Stati membri. In ambito sanitario, questo processo si è manifestato principalmente attraverso, da un lato, un'attività normativa vincolante fondata sulla base giuridica del mercato interno e, dall'altro, un filone giurisprudenziale che avvalla l'interpretazione ampia delle competenze dell'Unione [42]. Tale tendenza si conferma anche e soprattutto nel settore della sanità digitale, in cui l'utilizzo e l'interpretazione funzionale delle competenze non si sono limitati a quelle in materia di mercato interno (sezione 2.1), ma anche a quelle relative alla protezione e libera circolazione dei dati personali (sezione 2.2).

2.1. L'art. 114 TFUE: *longa manus* dell'Unione per intervenire in materia di sanità pubblica

Nella storia del processo di integrazione europea, la base giuridica che consente l'adozione di misure per il buon funzionamento del mercato interno ha assunto fin dal principio un campo di applicazione pressoché illimitato [43],

[41] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[42] Secondo la categorizzazione fornita da Garben, la modalità di integrazione a cui facciamo riferimento può essere ricondotta alla legislazione indiretta (o approccio "*cross-cutting*") e all'integrazione negativa della Corte. Cfr. S. GARBEN, *op. cit.*, 2019, p. 205 ss.

[43] R. SCHÜTZE, *op. cit*., 2021, p. 235. Si rinvia anche a R. BARENTS, *The Internal Market Unlimited: Some Observations on the Legal Basis of Community Legislation*, in *CMLRev.*,

conferendo così alla Comunità "*a factual Kompetenz-Kompetenz*" [44] che si estende anche a settori (almeno formalmente) di competenza nazionale. Se consideriamo vari ambiti del settore sociosanitario, le competenze degli Stati membri sono state interessate da un graduale processo di erosione. Nonostante i limiti stabiliti dai Trattati [45], sono numerosi gli esempi di atti che, pur avendo quale "centro di gravità" la tutela della salute umana, sono stati adottati facendo leva sulla competenza dell'Unione in materia di mercato interno [46].

L'estensione dell'applicazione delle regole sul mercato interno al settore sanitario [47] rende i confini formali di separazione delle competenze tra Unione e Stati membri più flessibili. In questo processo di allentamento delle maglie del sistema di ripartizione delle competenze, la Corte ha svolto un ruolo determinante [48], adottando un approccio generale di "*competence-*

1993, vol. 30, n. 1, pp. 87-88; B. DE WITTE, *Exclusive Member States Competences: Is there Such a Thing?*, in I. GOVAERE, S. GARBEN (eds.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Hart Publishing, Oxford, 2017, p. 59; P. CRAIG, G. DE BÚRCA, *EU Law: Text, Cases, and Materials*, OUP, Oxford, 2020, p. 127.

[44] R. BARENTS, *op. cit.*, 1993, p. 108.

[45] Secondo C. BARNARD, O. ODUDU, *op. cit*., 2009, "*the outer limits of the Treaty's power*" non hanno precluso alle regole del mercato interno di vincolare l'attività legislativa nazionale.

[46] Si pensi, ad esempio, ai regolamenti sulle qualifiche professionali (sanitarie), sui farmaci, sulla produzione e sulla pubblicità del tabacco, sulla fornitura di assistenza sanitaria transfrontaliera e sulla valutazione delle tecnologie sanitarie (v. T. HERVEY, A. DE RUIJTER, *The Dynamic Potential of European Union Health Law*, in *Eur. J. Risk Regul*., 2020, vol. 11, n. 4, pp. 726-35). L'adozione di tali misure è stata favorita dalla presenza di clausole come quella contenuta all'art. 114, par. 3, TFUE. In conformità con il principio *Health in All Policies* (HIAP) (art. 9 TFUE), questa clausola impone alla Commissione di garantire un elevato livello di protezione della sanità pubblica nel proporre atti per il ravvicinamento delle disposizioni nazionali che riguardano l'instaurazione e il buon funzionamento del mercato interno.

[47] F. COSTAMAGNA, *I servizi socio-sanitari nel mercato interno europeo. L'applicazione delle norme dell'Unione europea in materia di concorrenza, aiuti di Stato e libera circolazione dei servizi*, Edizioni Scientifiche Italiane, Napoli, 2011, p. 17. A questo riguardo, l'A. parla di una vera e propria "infiltrazione della disciplina relativa al mercato interno".

[48] Sull'influenza della Corte circa il riparto delle competenze, non solo in ambito sanitario, Di Federico individua sette tecniche adoperate dai giudici per ampliare la portata del diritto dell'Unione, tra cui l'affermarsi di un'accezione totalizzante dell'effetto utile e l'abbandono dell'elemento transfrontaliero come condizione necessaria per l'applicazione del diritto dell'Unione. Cfr. G. DI FEDERICO, *Principio di attribuzione e competenze esclusive degli Stati tra mito e realtà* (in corso di pubblicazione). Per ulteriori riferimenti dottrinali sul ruolo proattivo della Corte nell'ordinamento europeo, si rinvia anche a T. HORSLEY, *The Court of Justice of the European Union as an Institutional Actor. Judicial Lawmaking and its Limits*, CUP, Cambridge, 2022, p. 194; T. HORSLEY, *Reflection on the Role of the Court of Justice as the "Motor" of European Integration: Legal Limits to Judicial Lawmaking*, in *CMLRev.*, 2013, vol. 50, n. 4, p. 931; M. CAPPELLETTI, *Is the European Court of Justice Running Wild?*, in *Eur. Law Rev.*, 1987, vol. 12, pp. 3-17; L. AZOULAI, *The "Retained Powers" Formula in the*

enhancing" piuttosto che "*competence-restricting*" [49].

Un'eccezione che conferma la regola è rappresentata dalla sentenza *Tobacco Advertising* [50], con cui la Corte ha annullato, per la prima volta, un atto di diritto derivato (direttiva 98/43/CE) [51], adottato sulla base dell'art. 100A (oggi, art. 114 TFUE). La Corte, in un esercizio di "*judicial defence of the limits of EU legislative competence*" [52], ha ritenuto non adeguato il fondamento normativo della direttiva in questione, rilevando come quest'ultima non potesse dirsi effettivamente volta al miglioramento del mercato interno [53]. Nel giungere a tale conclusione, i giudici hanno definito il perimetro di applicazione dell'art. 100A in termini restrittivi, garantendo il rispetto dei limiti imposti dai Trattati [54].

In particolare, i giudici hanno affermato che l'art. 100A, pur potendo rappresentare la base giuridica di provvedimenti di armonizzazione con un'incidenza sulla protezione della salute umana [55], non può "aggirare l'esclusione

---

Case Law of the European Court of Justice: EU Law as Total Law?, in *Eur. J. Leg. Stud*., 2011, vol. 4, n. 2, p. 196; G. DAVIES, *Originalism at the European Court of Justice*, in I. GOVAERE, S. GARBEN (eds.), *The Internal Market 2.0*, Hart Publishing, Oxford, 2020, p. 323; G. DAVIES, *The European Union Legislature as an Agent of the European Court of Justice*, in *J. Common Mark. Stud*., 2016, vol. 54, p. 846; P. CRAIG, *The ECJ and the Ultra Vires Actions: a Conceptual Analysis*, in *CMLRev*., 2011, vol. 48, n. 2, p. 395; D. MARINES, *Judicial Influence on Policy Outputs? The Political Constraints of Legal Integration in the European Union*, in *Comparative Political Studies*, 2015, vol. 48, p. 1622; A.M. BURLEY, W. MATTLI, *Europe before the Court: A Political Theory of Legal Integration*, in *International Organization*, 1993, vol. 47, n. 1, pp. 41-76; P. SYRPIS, *The Relationship between Primary and Secondary Law in the EU*, in *CMLRev*., 2015, vol. 52, n. 2, p. 462; S. PRECHAL, S. DE VRIES, H. VAN EIJKEN, *The Principle of Attributed Powers and the "Scope of EU Law"*, in L.F.M. BESSELINK, F. PENNINGS, S. PRECHAL (eds.), *The Eclipse of the Legality Principle in the European Union*, Kluwer Law, Alphen aan den Rijn, 2011, p. 246; T.M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno*, Cacucci, Bari, 2018, p. 67; A. PISAPIA, *La base giuridica per l'adozione degli atti dell'Unione*, in *SIE*, 2017, n. 3, p. 659.

[49] S. WEATHERILL, *op. cit*., 2009, p. 20.

[50] Sentenza della Corte del 5 ottobre 2000, causa C-376/98, *Germania c. Parlamento europeo e Consiglio (Tobacco Advertising)*, EU:C:2000:544.

[51] Direttiva del Parlamento europeo e del Consiglio 98/43/CE, sul ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di pubblicità e di sponsorizzazione a favore dei prodotti del tabacco.

[52] S. WEATHERILL, *The Limits of Legislative Harmonization Ten Years after* Tobacco Advertising*: How the Court's Case Law has become a "Drafting Guide"*, in *Ger. Law J*., 2011, p. 830.

[53] Sentenza *Tobacco Advertising*, punti 90-118.

[54] R. SCHÜTZE, *Limits to the Union's 'Internal Market' Competence(s): Constitutional Comparisons*, in L. AZOULAI (ed.), *The Question of Competence in the European Union*, OUP, Oxford, 2014, p. 228.

[55] Sentenza *Tobacco Advertising*, punto 78.

di qualsiasi armonizzazione" stabilita dall'art. 129, n. 4, primo trattino, TCE (oggi, art. 168, par. 5, TFUE) [56].

La base giuridica del mercato interno, dunque, non deve essere interpretata in modo da attribuire all'Unione una "competenza generale a disciplinare il mercato interno" [57]. Il suo utilizzo deve invece essere limitato all'adozione di atti che hanno effettivamente per oggetto il miglioramento delle condizioni di instaurazione e di funzionamento del mercato interno [58]. Argomentare il contrario non solo non sarebbe conforme al principio di attribuzione [59], su cui si fonda l'ordinamento giuridico europeo, ma determinerebbe anche una violazione del divieto di armonizzazione di cui all'art. 129, n. 4, primo trattino, TCE [60]. L'applicazione rigorosa di tale principio impone alla Corte di fissare "*staging points, boundaries, clear demarcation lines, to EC expansion by way of positive law*" [61]. Come noto, tuttavia, questo approccio interpretativo non ha avuto fortuna.

La giurisprudenza successiva ha contribuito a legittimare la tendenza del legislatore europeo a perseguire "*non-market values in internal market legislation*" [62]. Sono diverse le occasioni in cui la Corte ha avallato la scelta del legislatore di utilizzare la propria competenza in materia di mercato interno per giustificare l'adozione di atti con un'incidenza in ambiti di prerogativa nazionale. Tra gli esempi più noti si possono ricordare la direttiva 2003/33/CE sulla pubblicità e sponsorizzazione a favore dei prodotti del tabacco [63] e la direttiva 2001/37/CE sulla lavorazione, presentazione e vendita di tali prodotti [64], poi abrogata dalla direttiva 2014/40/UE [65].

---

[56] *Ibid.* punto 79.

[57] *Ibid.* punto 83.

[58] *Ibid.* punto 84.

[59] Artt. 5, par. 1 e 4, par. 1, TUE, nonché la dichiarazione n. 18 relativa alla delimitazione delle competenze.

[60] Sentenza *Tobacco Advertising*, punto 83.

[61] S. DOUGLAS-SCOTT, *Constitutional Law of the European Union*, Pearson Education Limited, London, 2002, pp. 168-169. Pareri favorevoli rispetto alla pronuncia della Corte sono stati espressi anche, *inter alia*, da: B. DE WITTE, *A Competence to Protect: The Pursuit of Non-market Aims Through Internal Market Legislation*, in P. SYRPIS, *The Judiciary, the Legislature and the Internal Market*, CUP, Cambridge, 2012, p. 27 ss.; S. WEATHERILL, *op. cit*., 2011, p. 830; K. KONSTATINIDES, *Division of Powers in European Union Law – The Delimitation of Internal Competence between the EU and the Member States*, Kluwer Law International, Alphen aan den Rijn, 2009, p. 189.

[62] B. DE WITTE, *op. cit*., 2012, p. 25 ss.

[63] Sentenza della Corte del 12 dicembre 2006, causa C-380/03, *Repubblica di Germania c. Parlamento e Consiglio*, ECLI:EU:C:2006:772.

[64] Sentenze della Corte del 14 dicembre 2004, causa C-210/03, *Swedish Match*, ECLI:EU:C:2004:802, punti 27-58 e del 14 dicembre 2004, causa C-434/02, *Arnold André*, ECLI:EU:C:2004:800, punti 29-56.

[65] Sentenze della Corte del 4 maggio 2016, causa C-358/14, *Polonia c. Parlamento e Consiglio*, ECLI:EU:C:2016:323, punti 31-70; del 4 maggio 2016, causa C-477/14, *Pillbox*,

Anche in forza dell'interpretazione ampia della Corte riguardo all'ambito di applicazione dell'art. 114 TFUE, la Commissione non ha esitato a proporre nel 2004 di includere i servizi sanitari nel quadro normativo definito dalla direttiva Bolkestein sui servizi nel mercato interno [66]. Questa proposta, però, ha incontrato una forte opposizione degli Stati membri, che si sono fatti portavoce della difesa delle competenze loro attribuite dai Trattati. Grazie a un'intensa attività di lobbying condotta durante l'iter legislativo, i servizi sanitari sono stati esclusi dal campo di applicazione della direttiva [67], per essere successivamente disciplinati da una normativa *ad hoc*, la direttiva 2011/24/UE sui diritti dei pazienti [68]. Anche rispetto al contenuto di quest'ultima, gli Stati hanno esercitato un'influenza significativa [69], in reazione all'attivismo dei giudici della Corte in materia di mobilità transfrontaliera dei pazienti [70].

Nell'ambito di questo ampio e consolidato filone giurisprudenziale [71], la

---

ECLI:EU:C:2016:324, punti 123-124; del 4 maggio 2016, causa C-547/14, *Philip Morris*, ECLI:EU:C:2016:325, punti 54-64. Per ulteriori approfondimenti sulla giurisprudenza citata, cfr. S. WEATHERILL, *The Fundamental Question of Minimum and Maximum Harmonisation*, in I. GOVAERE, S. GARBEN (eds.), *op. cit*., 2020, p. 264 ss.; I. GOVAERE, *Internal Market Dynamics: On Moving Targets, Shifting Contextual Factors and the Untapped Potential of Article 3(3) TEU*, in I. GOVAERE, S. GARBEN (eds.), *op. cit*., 2020, p. 89 ss.

[66] Art. 23 proposta di direttiva del Parlamento europeo e del Consiglio relativa ai servizi nel mercato interno [SEC(2003) 21], COM(2004) 0002 final, del 25 febbraio 2004.

[67] Art. 2, par. 2, lett. f), e considerando 22-23 direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno.

[68] Direttiva 2011/24/UE del Parlamento europeo e del Consiglio del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera. Per un'analisi complessiva della direttiva 2011/24/UE, cfr. G. DI FEDERICO, *La direttiva 2011/24/UE e l'accesso alle prestazioni mediche nell'Unione europea,* in *Rivista di diritto della sicurezza sociale*, 2012, vol. 15, n. 3, pp. 683-704; F. COSTAMAGNA, *op. cit*., 2011, p. 210 ss.; M. INGLESE, *Le prestazioni sanitarie transfrontaliere e la tutela della salute*, in *Diritto comunitario e degli scambi internazionali*, 2012, vol. 51, pp. 109-138; M. PEETERS, *Free Movement of Patients: Directive 2011/24 on the Application of Patients' Rights in Cross-Border Healthcare*, in *Eur. J. Health Law*, 2012, vol. 19, n. 1, pp. 29-60.

[69] Occorre precisare, tuttavia, che il contenuto della direttiva è il risultato del bilanciamento non solo degli interessi fatti valere dagli Stati, ma anche di quelli rappresentati dal Parlamento europeo (rafforzamento dei diritti dei pazienti) e dalla Commissione (avanzamento del processo di integrazione europea rispetto ad alcuni aspetti connessi all'assistenza sanitaria) (F. COSTAMAGNA, *op. cit*., 2011, p. 239).

[70] A. DEN EXTER, A. SANTUARI, T. SOKOL, *One Year after the EU Patient Mobility Directive: A Three-Country Analysis*, in *Eur. Law Rev*., 2015, vol. 40, n. 2, p. 280.

[71] Cfr. C. NEWDICK, *The European Court of Justice, Trans-National Health Care and Social Citizenship – Accidental Death of a Concept?*, in *Wis. Int'l L.J.*, 2009, vol. 26, p. 867; S.L. GREER, *Migration of Patients and Migration of Power: Politics and Policy Consequences of Patient Mobility in Europe*, in *Wis. Int'l L.J*., 2009, vol. 26, n. 3, p. 910; G. DI FEDERICO, *Access to Healthcare in the Post-Lisbon Era and the Genuine Enjoyment of EU Citizens' Rights*, in L.S. ROSSI, F. CASOLARI (eds.), *The EU After Lisbon. Amending or Coping with the*

Corte ha adottato un approccio funzionalista basato sull'applicazione delle norme del mercato interno ai servizi sociosanitari nel contesto della libera circolazione delle merci e dei servizi [72]. Tale orientamento ha contribuito a superare i confini posti dai Trattati "*with a detrimental impact on the vertical distribution of competences between the Union and Member States*" [73]. Particolarmente esplicative dell'approccio interpretativo adottato sono le conclusioni dell'Avvocato generale Tesauro nelle cause *Decker* e *Kohll* [74], che sono state accolte dai giudici della Corte e seguite dalla giurisprudenza

Existing Treaties?, Springer, Cham, 2014, p. 184 ss.; A.J. OBERMAIER, *The End of Territoriality? The Impact of ECJ Rulings on British, German and French Social Policy*, Ashgate, Aldershot, 2009; S.L. GREER, S. RAUSHER, *Destabilization Rights and Restabilization Politics: Policy and Political Reactions to European Union Healthcare Services Law*, in *J. Eur. Public Policy*, 2011, vol. 18, pp. 220-240; T. HERVEY, *The European Union and the Governance of Health Care*, in G. DE BÚRCA, J. SCOTT, (eds.), *Law and New Governance in the EU and the US*, Hart Publishing, Oxford, 2006, pp. 179-210; W. PALM, I.A. GLINOS, *Enabling Patient Mobility in the EU: Between Free Movement and Coordination*, in E. MOSSIALOS et al. (eds.), *Health Systems Governance in Europe: The Role of European Union Law and Policy*, CUP, Cambridge, 2010, pp. 509-560; J. BAQUERO CRUZ, *The Case Law of the European Court of Justice on the Mobility of Patients: An Assessment*, in J.W. VAN GRONDEN et al. (eds.), *Health Care and EU Law*, Springer, The Hague, 2011, pp. 79-102; M. INGLESE, *op. cit.*, 2012, pp. 109-138. In particolare, per un'analisi degli effetti della giurisprudenza della Corte sull'autonomia degli Stati membri nella definizione della loro politica sanitaria, nonché nell'organizzazione e nella fornitura di servizi sanitari e di assistenza medica, si rinvia, *inter alia*, a P. CABRAL, *Cross-Border Medical Care in the European Union – Bringing Down a First Wall*, in *Eur. Law Rev*., 1999, vol. 24, n. 4, pp. 387-395; A. DAWES, *'Bonjour Herr Doctor': National Healthcare Systems, the Internal Market and Cross-Border Medical Care within the European Union*, in *Legal Issues of Economic Integration*, 2006, vol. 33, n. 2, pp. 167-182; R. CISOTTA, *Principi giurisprudenziali e nuove iniziative della Commissione in materia di patient mobility nell'Unione europea: un piccolo (o grande?) terremoto è in atto*, in *SIE*, 2007, vol. 3, pp. 161-82; C.M. RIEDER, *Cross-Border Movement of Patients in the EU: A Re-Appraisal*, in *Eur. J. Health Law*, 2017, vol. 24, n. 4, pp. 390-413; L. BUSATTA, *Moving Patients and Families and the Social Rights to Cross-Border Healthcare*, in M. PASCUAL, A. PÉREZ (eds.), *The Right to Family Life in the European Union*, Routledge, London, 2017, pp. 199-213.

[72] S.L. GREER, *op. cit.*, 2006, p. 143.

[73] T. HORSLEY, *op. cit*., 2022, p. 201. L'A. nota come "*[t]he case law on the reimbursement of the costs of medical treatments received abroad […] exemplifies the Court's use of directly effective EU norms to circumvent Member State efforts to impose express limits on Union legislative policymaking in specific policy areas*".

[74] Conclusioni dell'Avvocato generale Tesauro del 16 settembre 1997, cause C-120/95 e C-158/96, *Decker e Kohll*, ECLI:EU:C:1997:399. In dottrina, *Decker* e *Kohll* vengono individuati come "snodo fondamentale nell'affermazione del diritto di ottenere prestazioni sanitarie in uno Stato membro diverso da quello di affiliazione" (G. DI FEDERICO, S. NEGRI, *op. cit*., 2019, p. 41). Per alcuni, tali pronunce avrebbero addirittura acquisito un vero e proprio "*status of catechism*" nell'ordinamento europeo (G. DAVIES, *Welfare as a Service*, in *Legal Issues of Economic Integration*, 2002, vol. 29, n. 1, p. 28).

successiva [75]. In questa occasione, l'Avvocato generale ha affermato che la competenza esclusiva degli Stati nella configurazione dei loro sistemi previdenziali "non implica affatto che il settore previdenziale costituisca un'isola impermeabile all'influenza del diritto comunitario e che, di conseguenza, esulino dal suo campo di applicazione tutte le normative ad esso afferenti" [76]. Secondo l'Avvocato generale, il fatto che gli Stati abbiano il controllo sulla configurazione del sistema previdenziale nazionale non giustifica la violazione del principio fondamentale della libera circolazione delle persone [77]. Pertanto, le misure nazionali riguardanti la materia previdenziale non possono introdurre "restrizioni ingiustificate alla libera circolazione delle persone (stabilimento e servizi) e delle merci" [78].

Sulla base di queste argomentazioni, la Corte ha individuato le condizioni (procedurali e sostanziali) che uno Stato membro deve soddisfare affinché l'obbligo di autorizzazione preventiva al rimborso di cure mediche ricevute all'estero possa dirsi necessario e proporzionato rispetto all'obiettivo di interesse generale rappresentato dalla tutela della stabilità finanziaria del sistema sanitario [79]. Alcune di queste condizioni sono state oggetto di aspre critiche

---

[75] Sentenze della Corte, *Kohll*, punto 19 e *Decker*, punti 23-25; sentenze della Corte del 27 gennaio 2011, causa C-490/09, *Commissione c. Lussemburgo*, ECLI:EU:C:2011:34, punto 32; del 27 ottobre 2011, causa C-255/09, *Commissione c. Portogallo*, ECLI:EU:C:2011:695, punto 48; del 5 ottobre 2010, causa C-173/09, *Elchinov*, ECLI:EU:C:2010:581, punto 40; del 5 ottobre 2010, causa C-512/08, *Commissione c. Francia*, ECLI:EU:C:2010:579, punto 29; dell'11 settembre 2008, causa C-141/07, *Commissione c. Germania*, ECLI:EU:C:2008:492, punto 23; del 16 maggio 2006, causa C-372/04, *Watts*, ECLI:EU:C:2006:325, punto 92; del 18 marzo 2004, causa C-8/02, *Leichtle*, ECLI:EU:C:2004:161, punto 29; del 13 maggio 2003, causa C-385/99, *Müller-Fauré e van Riet*, ECLI:EU:C:2003:270, punto 100; del 23 ottobre 2003, causa C-56/01, *Inizan*, ECLI:EU:C:2003:578, punto 17; del 12 luglio 2001, causa C-157/99, *Smits e Peerbooms*, ECLI:EU:C:2001:404, punti 44-46.

[76] Conclusioni dell'Avvocato generale Tesauro in *Decker* e *Kohll*, punto 17.

[77] *Ibid.* punto 19.

[78] *Ibid.* punto 23. Per l'Avvocato generale, gli Stati membri sono tenuti a rispettare il diritto comunitario anche nell'esercizio della loro competenza in materia previdenziale, a meno che l'applicazione del diritto comunitario sia "tale da mettere in crisi la sopravvivenza dei regimi previdenziali". Di conseguenza, non è ammessa sul territorio nazionale alcuna discriminazione tra cittadini sulla base della nazionalità, salvo che la normativa nazionale sia "intimamente connessa al funzionamento e alla sopravvivenza del regime previdenziale" (punto 22). L'Avvocato generale sottolinea che "la circostanza che gli Stati membri, allo stato attuale, conservino intatta la propria competenza in materia previdenziale, così come in altre materie, non è sicuramente tale da consentire loro di adottare, nella materia di cui si tratta, normative che violino il diritto comunitario" (punto 25).

[79] Per un esame analitico del controllo procedurale e sostanziale della Corte rispetto alle misure derogatorie nazionali, si rinvia all'analisi di F. COSTAMAGNA, *op. cit.*, 2011, p. 159 s. L'A. evidenzia come, quanto al primo aspetto, la Corte richiede di valutare: 1) se il regime autorizzatorio sia fondato su criteri oggettivi, non discriminatori e noti in anticipo all'interessato (sentenza

da parte della dottrina, in quanto ritenute espressive di un'ingerenza indebita nella competenza esclusiva degli Stati membri [80]. Particolarmente controverso è, ad esempio, il riferimento alla "scienza medica internazionale" quale parametro per determinare l'ammissibilità di un trattamento sanitario ai fini del rimborso [81]. Secondo Costamagna, tale criterio risulta "difficilmente conciliabile con l'assunto secondo cui il diritto dell'Unione non può imporre agli Stati di ampliare l'elenco delle prestazioni prese a carico dai loro sistemi sanitari, il quale costituisce un corollario del principio, stabilito dall'articolo 168, par. 7, TFUE" [82].

2.2. L'art. 16 TFUE: un ulteriore "grimaldello" per forzare le maglie del sistema di competenze

Benché lontano dall'eguagliare per importanza la base giuridica relativa al mercato interno, anche solo per una questione temporale legata al suo ingresso nel quadro costituzionale dell'Unione, l'art. 16, par. 2, TFUE sta gradualmente assumendo una centralità crescente nell'ordinamento giuridico europeo. Viene infatti scelto – singolarmente o con altre norme di diritto primario – come fondamento normativo di un numero sempre maggiore di atti di diritto derivato dell'Unione [83]. Come illustreremo di seguito, alcune caratteristiche

Elchinov, punto 44); 2) se il procedimento previsto per il rilascio dell'autorizzazione sia facilmente accessibile agli interessati, la richiesta venga trattata entro tempi ragionevoli e in modo imparziale, nonché sia garantito l'accesso a un ricorso giurisdizionale effettivo avverso una decisione di diniego (sentenze *Smits e Peerbooms*, punto 90, *Müller-Fauré e Van Riet*, punto 85 e *Inizan*, punto 49). Per quanto riguarda, invece, il controllo sostanziale, i fattori da prendere in considerazione sono la tipologia (sentenza *Smits e Peerbooms*, punto 94) e la tempestività del trattamento rimborsabile (sentenze *Müller-Fauré e Van Riet*, punto 90 e *Watts*, punto 119). Cfr. G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, pp. 187-188.

[80] G. DI FEDERICO, *op. cit*., 2014, pp. 184-185, sottolinea come "*judgments as* Vanbraekel*,* Watts*, and* Elchinov *are likely to undermine national healthcare policies*". Nel primo caso, la Corte ha stabilito che l'istituzione competente dello Stato membro di affiliazione deve riconoscere al paziente il rimborso dell'eventuale differenza tra le spese sostenute per cure ospedaliere nello Stato di dimora e quelle che sarebbero state coperte nello Stato di affiliazione (sentenza *Vanbraekel*, punto 53). Nella sentenza *Watts*, inoltre, la Corte ha respinto l'argomentazione fatta valere dal governo inglese volta a giustificare le liste d'attesa come strumento di gestione dell'accesso alle prestazioni. Infine, in *Elchinov*, l'orientamento espresso dalla Corte ha indirettamente inciso sulla discrezionalità degli Stati membri nella definizione dei trattamenti rimborsabili, facendo leva sull'obbligo di interpretazione conforme.

[81] Sentenza *Smits e Peerbooms*, punto 94.

[82] F. COSTAMAGNA, *op. cit*., 2011, p. 169.

[83] Oltre allo EHDS, di recente, anche il regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza

intrinseche di questa disposizione, unite a significativi cambiamenti di contesto storico, inducono a ritenere che tale tendenza sia destinata a crescere nel tempo.

I primi atti legislativi fondati sull'art. 16, par. 2, TFUE sono stati il GDPR e la direttiva (UE) 2016/680 sulla protezione dei dati nell'attività di polizia giudiziaria (LED) [84]. A una prima analisi, entrambi questi strumenti sembrano essere stati adottati nel rispetto del riparto delle competenze tra l'Unione e gli Stati membri. Ciò si evince, in particolare, da due elementi. Il primo riguarda la scelta dello strumento giuridico utilizzato: da un lato un regolamento, che, come noto, permette di introdurre una normativa direttamente applicabile in tutti i suoi elementi, e, dall'altro, una direttiva che consente una maggiore flessibilità agli Stati membri nella scelta degli strumenti attraverso cui raggiungere gli obiettivi individuati dalla disciplina sovranazionale. La *ratio* che soggiace a tale scelta è evidente: la LED interviene, con un'armonizzazione minima [85], in una materia dove gli interessi nazionali hanno sempre avuto una certa rilevanza [86].

---

artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) ha come base giuridica gli artt. 16 e 114 TFUE.

[84] 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. La necessità di adottare una disciplina settoriale *ad hoc* per disciplinare i trattamenti nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia è stata espressa nella dichiarazione 21 allegata all'atto finale della Conferenza intergovernativa che ha adottato il Trattato di Lisbona. Gli obiettivi programmatici perseguiti dalla LED sono, da un lato, contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia che assicuri la libera circolazione dei dati tra le autorità competenti per finalità di applicazione normativa e, dall'altro, garantire un livello elevato di protezione di tali dati. Per un approfondimento sulla LED, v. E. KOSTA, F. BOEHM, *The EU Law Enforcement Directive (LED). A Commentary*, OUP, Oxford, 2024.

[85] All'art. 1, par. 3, direttiva (UE) 2016/680 viene infatti specificato che agli Stati non è preclusa la possibilità di prevedere garanzie più elevate di quelle stabilite nella direttiva per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti.

[86] A questo proposito, è opportuno ricordare che il regime precedente alla LED, rappresentato dalla decisione quadro 2008/977, riflettendo la struttura "a pilastri" dell'Unione prima dell'entrata in vigore del Trattato di Lisbona, lasciava "un ampio margine di manovra [agli] Stati membri". Cfr. documento di lavoro dei servizi della Commissione sulla valutazione d'impatto che accompagna il documento proposta di regolamento generale sulla protezione dei dati e proposta di direttiva concernente la tutela 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 di esecuzione di sanzioni penali, e la libera circolazione di

Il secondo elemento concerne invece il contenuto sostanziale degli strumenti normativi considerati. Innanzitutto, sia il GDPR sia la LED escludono dal proprio ambito di applicazione i trattamenti che riguardano la sicurezza nazionale, la quale, ai sensi dell'art. 4, par. 2, TUE, è di esclusiva competenza di ciascuno Stato membro [87]. A ciò si aggiunge la presenza di un numero significativo di ipotesi in cui la normativa sovranazionale riserva alla competenza statale il potere di legiferare, con la possibilità anche di prevedere deroghe ed esenzioni [88].

---

tali dati, SEC(2012) 73 final, del 25 gennaio 2012, p. 3; proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela 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, e la libera circolazione di tali dati, COM(2012) 10 final, del 25 gennaio 2012, p. 2.

[87] Cfr. art. 2, par. 2, e considerando 16 GDPR e art. 2, par. 3, LED.

[88] Nella LED, ad esempio, gli Stati membri possono adottare limitazioni ai diritti riconosciuti alle persone fisiche (ad es. diritto di accesso, di rettifica o cancellazione), facendo valere interessi, quali la sicurezza nazionale (artt. 15, par. 1 e 16, par. 4, LED). Ancor più emblematico, nel GDPR, è l'art. 85 GDPR che attribuisce al legislatore nazionale il compito di trovare il giusto equilibrio tra il diritto alla protezione dei dati personali e la tutela della libertà di manifestazione del pensiero e di informazione, compresa la libertà di espressione accademica, artistica e letteraria. Dal momento che simili operazioni di bilanciamento richiedono di tenere conto di differenze culturali e tradizioni nazionali che rientrano nella sfera identitaria di ciascuno Stato membro, il legislatore europeo – spesso su pressione degli stessi Stati membri – ha ritenuto di non poter imporre una regolazione uniforme, adottando di conseguenza interventi meno incisivi. Lo stesso avviene per i trattamenti di dati sanitari ai fini di ricerca scientifica, rispetto ai quali l'ampio margine di manovra concesso agli Stati membri trova giustificazione nel fatto che i settori sanitario e della ricerca rappresentano una prerogativa statale (art. 5, par. 1, lett. e), art. 9, par. 2, lett. j) e par. 4 e art. 89 GDPR). Se la tutela e il miglioramento della salute rientrano tra le competenze di supporto (art. 6, par. 1, lett. a), TFUE), la ricerca, pur apparendo nell'elenco delle competenze concorrenti, beneficia, insieme allo sviluppo tecnologico e allo spazio, dell'inoperatività della *preemption*. Ciò significa che l'intervento dell'Unione in tali settori non pregiudica la possibilità che gli Stati membri esercitino la loro competenza (art. 4, par. 3, TFUE). Per un approfondimento sul principio della *preemption*, cfr. D. CHALMERS, G. DAVIES, G. MONTI, *European Union Law. Cases and Materials*, CUP, Cambridge, 2010, pp. 206-207; R. SCHÜTZE, *Supremacy without Pre-emption? The Very Slowly Emergent Doctrine of Pre-emption*, in *CMLRev*., 2006, vol. 43, n. 4, pp. 1023-1048; A. ARENA, *Il principio della preemption in diritto dell'Unione europea. Esercizio delle competenze e ricognizione delle divergenze tra diritto derivato e diritto nazionale*, Editoriale scientifica, Napoli, 2013; A. ARENA, *Exercise of EU Competence and Pre-emption of Member States' Power in the Internal and External Sphere: Towards "Grand Unification"?*, in *Yearb. Eur. L.*, 2016, vol. 35, n. 1, p. 28; A. ARENA, *The Doctrine of Union Pre-emption in the EU Internal Market: Between Sein and Sollen*, in *Colum. J. Eur. L.*, 2010, vol. 17, p. 481; L. GORMLEY, *Free Movement of Goods and Pre-emption of State Power*, in A. ARNULL, C. BARNARD (eds.), *A Constitutional Order of States? Essays in EU Law in Honour of Alan Dashwood*, Bloomsbury Publishing, London, 2011, p. 365 ss.; S. WEATHERILL, *Pre-emption, Harmonization and Distribution of Competence to Regulate the Internal Market*, in C. BARNARD, J. SCOTT (eds.), *The Law of the Single Market. Unpacking the Premises*, Bloomsbury

L'art. 16, par. 2, TFUE, dunque, è stato utilizzato per adottare degli atti che, se letti attraverso la lente del principio di attribuzione, appaiono rispettosi del quadro costituzionale vigente. Ciò non toglie che la formulazione stringata e tutt'altro che chiara di tale disposizione si presti a operazioni interpretative particolarmente creative. Un caso esemplificativo in tal senso è quello del noto Parere 1/15 relativo all'accordo tra l'Unione e il governo del Canada sul trasferimento dei dati del codice di prenotazione (accordo PNR), rispetto a cui la Corte è chiamata a esprimersi su due profili. Uno relativo alla compatibilità dello stesso con i Trattati e, in particolare, con l'art. 16 TFUE e gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (Carta) [89]. L'altro, invece, sull'adeguatezza della base giuridica della decisione del Consiglio relativa alla conclusione dell'accordo PNR. Ai fini della presente analisi, ci concentreremo su quest'ultimo profilo, rispetto al quale è interessante considerare le diverse posizioni tenute dalle istituzioni europee: da un lato, il Parlamento europeo e, dall'altro, la Commissione e il Consiglio.

Il primo ritiene che la decisione del Consiglio sia stata fondata erroneamente sugli articoli relativi alla cooperazione giudiziaria e di polizia [90]. A suo avviso, infatti, la finalità e il contenuto principale di tale decisione sono la protezione dei dati personali e non la sicurezza e l'incolumità delle persone. Pertanto, il fondamento costituzionale corretto sarebbe dovuto essere l'art. 16 TFUE che, sostiene il Parlamento, si "applica a *tutti* i settori del diritto dell'Unione", inclusi quelli relativi allo spazio di libertà, sicurezza e giustizia [91].

Publishing, London, 2002, p. 41; E. CROSS, *Pre-emption of Member State Law in the European Economic Community: A Framework for Analysis*, in *CMLRev*., 1992, vol. 29, n. 3, p. 447; M. ORLANDI, *L'evoluzione del primato del diritto dell'Unione europea*, UTET Giuridica, Torino, 2012; S. DOUGLAS-SCOTT, *op. cit.*, 2002, pp. 168-169.

[89] Per un approfondimento del parere, si rinvia, *inter alia*, a C. KUNER, *International Agreements, Data Protection, and EU Fundamental Rights On The International Stage: Opinion 1/15, EU-Canada PNR*, in *CMLRev*., 2018, vol. 55, p. 876; H. HIELKE, *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, in *Eur. Data Protection L. Rev*., 2017, vol. 3, p. 410; C. KUNER, *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15*, in *Verfassungsblog*, 2017; C. DOCKSEY, *Opinion 1/15: Privacy and Security, Finding the Balance*, in *Maastricht J. Eur. &Comp. L*., 2017, vol. 24, p. 771.

[90] Art. 82, par. 1, comma 2, lett. d), e art. 87, par. 2, lett. a), TFUE, art. 82, par. 1, comma 2, lett. d), e art. 87, par. 2, lett. a), TFUE.

[91] Parere 1/15 della Corte, emesso ai sensi dell'art. 218, par. 11, TFUE, del 26 luglio 2017, ECLI:EU:C:2016:656, punto 32. Tuttavia, al punto 34, il Parlamento europeo riconosce che, qualora la Corte dovesse ritenere che le finalità perseguite dall'accordo siano tra loro inscindibili, la decisione del Consiglio relativa alla conclusione dell'accordo potrebbe legittimamente fondarsi congiuntamente sull'art. 16 TFUE, sull'art. 82, par. 1, comma 2, lett. d), TFUE e sull'art. 87, par. 2, lett. a), TFUE.

Il Consiglio e la Commissione, invece, sostengono che l'art. 16 TFUE possa fungere da base giuridica di un atto "*soltanto* qualora il suo obiettivo principale sia la protezione dei dati personali". Al contrario, se l'atto ha come finalità principale "la realizzazione di politiche settoriali" che implicano il trattamento di dati personali, la base giuridica adeguata dovrebbe essere quella corrispondente alla politica interessata, nel rispetto dell'art. 8 Carta e dell'art. 16 TFUE [92].

Tra queste due letture dell'art. 16, par. 2, TFUE, la Corte ha accolto quella del Parlamento europeo. Secondo i giudici di Lussemburgo, infatti, il ricorso all'art. 16, par. 2, TFUE costituisce una base giuridica adeguata "quando la protezione dei dati personali è *una delle* finalità o delle componenti essenziali" delle norme europee, comprese quelle relative alla cooperazione giudiziaria in materia penale e alla cooperazione di polizia [93]. Dalle brevi indicazioni fornite dalla Corte, quindi, l'ambito di applicazione dell'art. 16, par. 2, TFUE sembra dover essere inteso in senso ampio, comprendendo potenzialmente tutte le politiche dell'Unione, fatta eccezione per la politica estera e di sicurezza comune [94].

Una linea interpretativa analoga è stata seguita anche dall'Avvocato generale Szpunar nella causa *Österreichische Datenschutzbehörde c. WK* [95]. In questo caso, l'ambito di applicazione dell'art. 16, par. 2, TFUE è stato esteso sino a ricomprendere attività di controllo svolte da una commissione

---

[92] *Ibid.* punto 48. Sulla base di tali argomentazioni, il Consiglio e la Commissione concludono che la decisione dovrebbe fondarsi sulle disposizioni in materia di cooperazione giudiziaria e di polizia, dal momento che l'obiettivo principale è la sicurezza e l'incolumità delle persone, rispetto alle quali la protezione dei dati ha solamente carattere accessorio.

[93] *Ibid.* punto 96. Nel caso di specie, essendo la componente relativa alla tutela della sicurezza pubblica e quella della protezione dei dati PNR inscindibilmente connesse (punto 94) e non essendovi incompatibilità tra le procedure legislative in questione (punti 106 ss.), la base giuridica della decisione del Consiglio non può che essere rappresentata tanto dall'art. 16, par. 2, TFUE, quanto dall'art. 87, par. 2, lett. a), TFUE. Viene invece escluso dai giudici il ricorso all'art. 82, par. 1, comma 2, lett. d), TFUE, in assenza di disposizioni volte a facilitare la cooperazione giudiziaria (punti 102-103).

[94] È lo stesso art. 16, par. 2, TFUE a escludere la PESC dal proprio ambito di applicazione, lasciando che sia l'art. 39 TUE a rappresentare il fondamento giuridico degli atti relativi ai trattamenti di dati personali in questo settore specifico.

[95] Conclusioni dell'Avvocato generale Szpunar dell'11 maggio 2023, causa C-33/22, *Österreichische Datenschutzbehörde c. WK*, ECLI:EU:C:2023:397. Sebbene in questo lavoro ci si concentri sull'analisi delle conclusioni dell'Avvocato generale, va detto che la Corte, aderendo alla linea interpretativa proposta da Szpunar, ha risposto affermativamente a entrambi i quesiti posti dal giudice del rinvio (sentenza della Corte del 16 gennaio 2024, causa C-33/22, *Österreichische Datenschutzbehörde*, ECLI:EU:C:2024:46). Per un commento, cfr. M. SZYDŁO, *How Should the EU Protect Personal Data without Undermining the Essential Functions of Member States and their Constitutional Principles?* Österreichische Datenschutzbehörde v. WK, in *CMLRev*, 2024, vol. 61, n. 5, pp. 1367-1388.

parlamentare di inchiesta di uno Stato membro, sebbene l'inchiesta in oggetto riguardasse questioni relative alla sicurezza nazionale [96]. Ciò avviene in ragione di un'interpretazione "generalizzante" dell'art. 16, par. 2, TFUE, per cui rientrano "nell'ambito di applicazione del diritto dell'Unione", ai sensi dell'art. 16, par. 2, TFUE, le attività che "*possono* rientrarvi, nel senso che non sono state sottratte ad esso in ragione delle competenze esclusive degli Stati membri" [97]. Secondo l'Avvocato generale, infatti, stabilire un legame concreto tra il trattamento dei dati personali e disposizioni specifiche del diritto dell'Unione sarebbe troppo complicato per via "della specificità dei dati

[96] Sulla crescente influenza esercitata in questo settore da parte dell'Unione, si rinvia all'analisi di F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revised*, in *Eur. Foreign Aff. Rev.*, 2023, vol. 28, n. 4, pp. 323-340, dove si evidenzia come la "dottrina sull'autonomia strategica" stia contribuendo a ridefinire i contorni del sistema di competenze. Nella stessa direzione si colloca il contributo di C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO, *La trasformazione digitale in Europa. Diritti e principi*, Giappichelli, Torino, 2023, p. 9 ss., in cui si mette in luce come "in diverse pronunce della Corte di giustizia determinate esigenze di sicurezza nazionale sono state subordinate alla necessità di garantire che le disposizioni di atti legislativi UE strumentali alla transizione digitale siano interpretate in modo da soddisfare altre priorità, come alcuni diritti fondamentali". Al riguardo, vengono citate le decisioni che sono ricondotte alla c.d. "saga" sulla *data retention*, ossia le sentenze della Corte del 2 marzo 2021, causa C-746/18, *H.K. c. Prokuratuur*, ECLI:EU:C:2021:152; del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a*., ECLI:EU:C:2020:791; del 6 ottobre 2020, causa C-623/17, *Privacy International*, ECLI:EU:C:2020:790; del 21 dicembre 2016, causa C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970; del 6 ottobre 2015, causa C-362/14, *Schrems I*, ECLI:EU:C:2015:650; dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238. Cfr. M. TZANOU, P. VOGIATZOGLOU, *National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach*, in *European Papers*, 2025, vol. 10, n. 3, pp. 803-836.

[97] Conclusioni dell'Avvocato generale in *Österreichische Datenschutzbehörde c. WK*, punto 50. Al contrario, la lettura "concretizzante", accolta dal giudice del rinvio, equipara l'"ambito di applicazione del diritto dell'Unione" all'espressione "attuazione del diritto dell'Unione" di cui all'art. 51, par. 1, Carta. Sulla base di tale interpretazione, il giudice del rinvio ritiene che il GDPR sia inapplicabile al caso concreto, in quanto le attività di un organo parlamentare con funzioni di controllo politico non sono disciplinate da alcuna disposizione del diritto dell'Unione, ma solamente da norme di diritto nazionale. A suo avviso, infatti, queste attività "si collocano al centro dell'attività del Parlamento" (punto 25) e, quindi, non dovrebbero poter essere ricomprese nell'ambito del diritto dell'Unione, a differenza, invece, di attività della commissione per le petizioni del Parlamento, rispetto alle quali la Corte ha riconosciuto l'applicabilità del GDPR in *Land Hessen* (sentenza della Corte del 9 luglio 2020, causa C-272/19, *Land Hessen*, ECLI:EU:C:2020:535). In quel caso, il Presidente del Parlamento aveva negato l'accesso ai dati richiesto da un cittadino nell'ambito di una petizione, sostenendo che si trattasse di un'attività parlamentare non soggetta al GDPR. In senso critico rispetto al ragionamento svolto dai giudici della Corte, cfr. R. POSNIK, *Legal Considerations on the CJEU Judgment of 9 July 2020, C-272/19*, in *International Journal of Parliamentary Studies*, 2021, vol. 1, pp. 154-159.

personali, la cui circolazione e il cui sfruttamento sono facilitati dalla loro digitalizzazione" [98].

Accogliere un'interpretazione così ampia dell'art. 16, par. 2, TFUE risulta problematico. Il fatto di non richiedere l'esistenza di un nesso diretto tra le attività di trattamento dei dati e l'applicazione del diritto dell'Unione amplia notevolmente il novero di situazioni rispetto alle quali è possibile ricorrere all'art. 16, par. 2, TFUE. Se con "ambito di applicazione del diritto dell'Unione" si intende – sostanzialmente – "ambito di competenza dell'Unione" [99], ciò significa che l'art. 16, par. 2, TFUE può costituire la base giuridica per qualunque atto normativo che riguarda una materia compresa tra quelle di competenza esclusiva (formale o per esercizio) [100], anche laddove la protezione dei dati personali rappresenti una componente accessoria.

Inoltre, altri fattori contribuiscono a legittimare un utilizzo di tale base giuridica trasversale a tutte le politiche europee (approccio "*cross-cutting*") [101]. In primo luogo, risulta evidente che attualmente nessuna politica può dirsi

---

[98] *Ibid.* punto 44. Nello specifico, l'Avvocato generale stabilisce che le attività della commissione parlamentare d'inchiesta siano soggette al GDPR, perché, secondo la ripartizione delle competenze tra Unione e Stati membri, le attività di mero controllo non sono di riserva esclusiva degli Stati (punti 102-104). A riprova dell'esistenza di un concorso di competenza in materia, viene ricordata la duplicazione delle indagini sul "Dieselgate" a opera del Parlamento federale tedesco e del Parlamento europeo, tramite l'adozione della decisione (UE) 2016/34 sulla costituzione, le attribuzioni, la composizione numerica e la durata del mandato della commissione d'inchiesta sulla misurazione delle emissioni nel settore automobilistico. Inoltre, l'Avvocato generale osserva che tali attività devono considerarsi regolate dal GDPR, in quanto non sono escluse in modo esplicito dall'art. 2, par. 2, GDPR (punto 102). In linea con quanto affermato dalla Corte in *Land Hessen*, l'eccezione di cui all'art. 2, par. 2, lett. a), GDPR deve essere interpretata in senso restrittivo: ne consegue che sono sottratte all'applicazione del GDPR solo le attività espressamente menzionate in tale disposizione o assimilabili, indipendentemente che si tratti di attività dello Stato o di una pubblica autorità (punto 56).

[99] Tale interpretazione si colloca nel solco della giurisprudenza della Corte che ha adottato una lettura estensiva dell'ambito di applicazione della Carta come definito dall'art. 51 della stessa (Cfr. J. ZILLER, *Art. 51*, in R. MASTROIANNI, *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017, pp. 1052-1056). Tuttavia, non occorre ricordarlo, l'art. 16, par. 2, TFUE non coincide con l'art. 8 della Carta sul diritto alla protezione dei dati personali. Di conseguenza, adottare la medesima linea interpretativa non appare del tutto corretto.

[100] Rifacendosi a una categoria nota nel periodo precedente a Lisbona, sono materie rispetto a cui l'Unione esercita una competenza esclusiva "per esercizio" sia quelle elencate all'art. 3 TFUE sia quelle previste dall'art. 4 TFUE, qualora l'Unione abbia esercitato la propria competenza. Cfr. E. CANNIZZARO, *op. cit.*, 2022, p. 273.

[101] La materia della protezione e della libera circolazione dei dati personali condivide il carattere tipico di altre competenze orizzontali, come quella in materia di mercato interno (S. WEATHERILL, *op. cit.*, 2020, p. 264 ss.) e di sanità pubblica (G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, p. 22). Tale natura trasversale emerge con particolare evidenza nel settore digitale, il quale "intercetta numerose politiche dell'Unione" e, conseguentemente, può fondarsi su un ampio spettro di basi giuridiche. Cfr. C. AMALFITANO, F. FERRI, *op. cit.*, 2023, p. 8.

esente dal processo di digitalizzazione in atto. Un numero significativo di attività economiche e sociali dipendono dalla raccolta e dalla condivisione di dati, il cui trattamento è facilitato dall'utilizzo di tecnologie avanzate (ad es. l'intelligenza artificiale) [102].

In secondo luogo, la competenza in materia di protezione dei dati personali interseca una vasta gamma di settori, in ragione della dimensione di diritto fondamentale che la caratterizza. Come stabilito da una giurisprudenza consolidata, ogni provvedimento adottato dalle istituzioni deve rispettare i diritti fondamentali dell'Unione e lo stesso vale per gli atti adottati dagli Stati membri nell'esecuzione di obblighi che derivano dal diritto dell'Unione o che ricadono nell'ambito di applicazione del diritto dell'Unione [103]. Ne consegue

---

[102] Già nel piano d'azione di attuazione del programma di Stoccolma, la Commissione sottolineava che "[i]n una società globalizzata, caratterizzata da un rapido progresso tecnologico in cui lo scambio d'informazioni non conosce confini, è quanto mai importante garantire il rispetto della vita privata. L'Unione deve assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati. Occorre rafforzare la posizione dell'UE in relazione alla protezione dei dati personali in tutte le politiche europee, anche nel contrastare e prevenire la criminalità e nelle relazioni internazionali". Cfr. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Creare uno spazio di libertà, sicurezza e giustizia per i cittadini europei. Piano d'azione per l'attuazione del programma di Stoccolma, COM(2010) 171 final, del 20 aprile 2010.

[103] V., *inter alia*, sentenze della Corte del 14 ottobre 2004, causa C-36/02, *Omega*, ECLI:EU:C:2004:614, punto 35; del 12 giugno 2003, causa C-112/00, *Schmidberger*, ECLI:EU:C:2003:333, punto 75; del 18 giugno 1991, causa C-260/89, *ERT*, ECLI:EU:C:1991:254, punti 42 ss. Sull'utilizzo della protezione dei diritti fondamentali come strumento per ampliare la sfera d'influenza dell'Unione, si rinvia a E. DUBOUT, *The Protection of Fundamental Rights and the Allocation of Competences in the EU: A Clash of Constitutional Logics*, in L. AZOULAI (ed.), *op. cit.*, 2014, pp. 193-211: l'A. mette in evidenza come l'obiettivo della tutela dei diritti fondamentali consente all'Unione di "*apply its fundamental rights in an increasing number of situations, even if such situations are outside the scope of its competences*". In questo processo di graduale applicazione dei diritti fondamentali, Dubout identifica tre fasi (pp. 194-195). La prima fase, coincidente con le pronunce *Stauder* (sentenza della Corte del 12 novembre 1969, causa C-29/69, ECLI:EU:C:1969:57) e *Internationale Handelsgesellschaft* (sentenza della Corte del 17 dicembre 1970, causa C-11/70, ECLI:EU:C:1970:114), in cui si afferma che gli atti e le istituzioni dell'Unione devono rispettare i diritti fondamentali. La seconda fase, riconducibile alle pronunce *Wachauf* (sentenza della Corte del 13 luglio 1989, causa C-5/88, ECLI:EU:C:1989:321) e *ERT*, secondo cui la giurisdizione della Corte relativa ai diritti fondamentali si estende anche alle misure nazionali che applicano o derogano il diritto dell'Unione. Infine, la terza fase è associata alle sentenze *Kücükdeveci* (sentenza della Corte del 19 gennaio 2010, causa C-555/07, ECLI:EU:C:2010:21) e *Zambrano* (sentenza della Corte dell'8 marzo 2011, causa C-34/09, ECLI:EU:C:2011:124), in cui il campo di applicazione dei diritti fondamentali viene esteso oltre alla loro sfera, incidendo anche su situazioni di competenza nazionale (v. sentenza della Corte del 22 dicembre 2010, causa C-208/09, *Sayn-Wittgenstein*, ECLI:EU:C:2010:806). Sul punto si veda anche V. KOSTA, *Fundamental Rights Mainstreaming in the EU*, in F. IPPOLITO, M.E. BARTOLONI, M. CONDINANZI, *op. cit*., 2019, p. 14 ss.

che atti di cui anche solo alcune disposizioni possono incidere sul diritto alla protezione dei dati personali potrebbero richiedere un ricorso all'art. 16, par. 2, TFUE.

È il caso, ad esempio, del regolamento sull'Intelligenza Artificiale (AIA) che, sebbene miri in larga parte a favorire l'istaurazione e il buon funzionamento del mercato unico digitale, contiene "regole specifiche sulla protezione delle persone fisiche per quanto concerne il trattamento di dati personali, in particolare, restrizioni all'utilizzo di sistemi di Intelligenza Artificiale (IA) per l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto" [104]. Questo, seppur tenue, collegamento con il diritto alla protezione dei dati personali giustifica, secondo il legislatore, il duplice fondamento giuridico negli artt. 114 e 16, par. 2, TFUE.

Lungo tale direttrice si colloca anche lo EHDS, in cui l'uso congiunto di basi giuridiche "forti" permette all'Unione di armonizzare un settore in cui un simile intervento non sarebbe formalmente consentito [105], sollevando non poche preoccupazioni quanto al (pieno) rispetto del quadro costituzionale esistente.

3. Una base giuridica "forte" per un'integrazione più profonda

Come noto, nell'ordinamento giuridico dell'Unione, fondato sul principio di attribuzione [106], qualsiasi atto destinato a produrre effetti giuridici deve, a pena di nullità, essere basato direttamente ("poteri conferiti") o indirettamente

---

[104] Punto 2.1 della proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final e considerando 3 del regolamento sull'IA.

[105] S. SLOKENBERGA, *Setting the Foundations: Individual Rights, Public Interest, Scientific Research and Biobanking*, in S. SLOKENBERGA, O. TZORTZATOU, J. REICHEL (eds.), *GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe*, Springer, Cham, 2021, p. 14.

[106] Cfr. parere 2/94 della Corte del 28 marzo 1996 sull'adesione della Comunità alla Convenzione dei diritti dell'uomo e delle libertà fondamentali, ECLI:EU:C:1996:140, in cui si afferma che l'ordinamento comunitario si basa sul principio dei poteri attribuiti (punto 4). Ciò significa che l'Unione può agire solo entro i limiti fissati dagli Stati membri, a meno che non operino deroghe o temperamenti di cui ai Trattati. Si pensi, ad esempio, alla c.d. clausola di flessibilità *ex* art. 352 TFUE che, al primo paragrafo stabilisce che: "[s]e un'azione dell'Unione appare necessaria, nel quadro delle politiche definite dai trattati, per realizzare uno degli obiettivi di cui ai trattati senza che questi ultimi abbiano previsto i poteri di azione richiesti a tal fine, il Consiglio, deliberando all'unanimità su proposta della Commissione e previa approvazione del Parlamento europeo, adotta le disposizioni appropriate".

("poteri delegati") su una specifica disposizione dei Trattati che ne rappresenti la base giuridica. Quest'ultima ha rilevanti implicazioni in termini di competenza sostanziale e di procedura, dal momento che determina le modalità di esercizio di tale competenza, indicando (talvolta) gli strumenti normativi da utilizzare e la procedura legislativa da seguire [107]. Per quanto riguarda il primo aspetto, la base giuridica chiarisce la ripartizione delle competenze tra l'Unione e gli Stati membri e il modo in cui l'Unione dovrebbe esercitarle nel rispetto dei principi di sussidiarietà e proporzionalità [108]. Per quanto riguarda il secondo aspetto, i requisiti procedurali stabiliti dalla base giuridica definiscono le forme e la portata della partecipazione istituzionale e le procedure di voto [109].

Data l'importanza costituzionale della base giuridica [110], la Corte ha individuato con precisione i criteri che dovrebbero orientare il legislatore nella scelta del fondamento costituzionale di un atto al fine, da un lato, di tenere conto degli obiettivi dei Trattati e, dall'altro, di preservare l'equilibrio interistituzionale [111]. Tale scelta, secondo la Corte, dovrebbe essere effettuata facendo riferimento a "elementi oggettivi, suscettibili di sindacato giurisdizionale", tra cui lo scopo dell'atto [112].

---

[107] K. LENAERTS, P. VAN NUFFEL, *European Union Law*, Sweet & Maxwell, London, 2011, pp. 113-114.

[108] Art. 5, parr. 3 e 4, TUE e Protocollo n. 2 sull'applicazione dei principi di sussidiarietà e di proporzionalità. Per una disamina dei principi in oggetto, si rinvia, *ex multis*, all'analisi di K. LENAERTS, *The Principle of Subsidiarity and the Environment in the European Union: Keeping the Balance of Federalism*, in *Fordham Int. Law J*., 1994, vol. 17, n. 4, p. 846; P. DE PASQUALE, *Il principio di sussidiarietà nell'ordinamento comunitario*, Editoriale scientifica, Napoli, 2000; U. VILLANI, *I principi di sussidiarietà e di proporzionalità nel diritto dell'Unione europea*, in L.F. PACE (a cura di), *Nuove tendenze del diritto dell'Unione europea dopo il Trattato di Lisbona*, Giuffrè, Milano, 2012, p. 79 ss.; G. DAVIES, *Subsidiarity: The Wrong Idea, in the Wrong Place, at the Wrong Time*, in *CMLRev*., 2006, vol. 43, n. 1, p. 63 ss.; M.C. CICIRIELLO, *L'Unione europea e i suoi principi giuridici*, Editoriale scientifica, Napoli, 2010; D.U. GALETTA, *Il principio di proporzionalità comunitario e il suo effetto spill over negli ordinamenti nazionali*, in *Nuove autonomie*, 2005, p. 541 ss.

[109] Sentenza della Corte del 1° ottobre 2009, causa C-370/07, *Commissione c. Consiglio*, ECLI:EU:C:2009:590, punti 48-49.

[110] Come sottolineato dalla Grande Sezione della Corte nel parere 1/15 sul progetto di accordo tra l'Unione europea e il Canada relativo al trasferimento dei dati del codice di prenotazione dei passeggeri aerei, "la scelta della base giuridica adeguata riveste un'importanza di natura costituzionale dato che l'Unione, disponendo soltanto di competenze di attribuzione, deve ricondurre gli atti che adotta alle disposizioni del Trattato FUE che l'abilitino effettivamente a tal fine" (punto 71).

[111] T.M. MOSCHETTA, *op. cit*., 2018, p. 73 ss.

[112] Sentenze della Corte del 16 febbraio 2022, causa C-156/21, *Ungheria c. Parlamento e Consiglio*, ECLI:EU:C:2022:97, punto 107; dell'8 dicembre 2020, causa C-626/18, *Polonia*

Per i fini di questa analisi, risulta quindi di particolare rilievo soffermarsi sugli obiettivi dello EHDS per verificare se quelli espressamente menzionati nel testo del regolamento siano quelli che effettivamente tale strumento normativo intende perseguire (sezione 3.1). In caso contrario, sarà evidente che la scelta del legislatore europeo di fondare lo EHDS sugli artt. 114 e 16, par. 2, TFUE sia motivata dall'esigenza di realizzare, secondo lo schema tipico della teoria neo-funzionalista, una maggiore integrazione nel settore della salute (sezione 3.2).

3.1. Gli obiettivi espliciti (e impliciti) dello spazio europeo dei dati sanitari

La creazione dello EHDS mira ad assicurare l'accesso e la trasmissione dei dati sanitari elettronici a livello nazionale e transfrontaliero per finalità di uso primario (ad es. l'assistenza sanitaria) e secondario (ad es. la ricerca scientifica), nel rispetto del GDPR qualora si tratti di dati sanitari elettronici personali [113]. Inoltre, lo EHDS punta a stabilire regole comuni per la realizzazione di un mercato unico delle cartelle cliniche elettroniche e delle applicazioni per il benessere [114]. Alla luce di tali obiettivi, esplicitamente menzionati all'art. 1 EHDS, non sorprende – almeno a un primo sguardo – che il fondamento costituzionale prescelto sia rappresentato dagli artt. 16, par. 2, e 114 TFUE.

Come evidenziato in precedenza, l'art. 16, par. 2, TFUE rappresenta una base giuridica adeguata "quando la protezione dei dati personali è *una delle* finalità o delle componenti essenziali" delle norme europee [115]. Con lo EHDS, tale finalità viene perseguita tramite l'introduzione di norme che specificano e integrano i diritti conferiti dal GDPR alle persone fisiche (ad es. il diritto di accesso, il diritto alla portabilità dei dati e il diritto di *opt-out*), rafforzando così il loro controllo sull'uso primario e secondario dei dati sanitari elettronici personali [116]. L'art. 16, par. 2, TFUE permette anche di giustificare l'adozione

---

c. Parlamento e Consiglio, ECLI:EU:C:2020:1000, punto 43; dell'8 dicembre 2020, causa C-620/18, *Ungheria c. Parlamento e Consiglio*, ECLI:EU:C:2020:1001, punto 38; del 3 dicembre 2019, causa C-482/17, *Repubblica ceca c. Parlamento e Consiglio*, ECLI:EU:C:2019:1035, punto 31; del 19 luglio 2012, causa C-130/10, *Parlamento c. Consiglio*, ECLI: EU:C:2012:472, punto 42; parere 1/15 della Corte, punto 76; del 26 marzo 1996, causa C-271/94, *Parlamento c. Consiglio*, ECLI:EU:C:1996:133, punto 14; del 17 marzo 1993, causa C-155/91, *Commissione c. Consiglio*, ECLI:EU:C:1993:98, punto 7.

[113] Art. 1, par. 2, lett. a) e c-e), EHDS.

[114] Art. 1, par. 2, lett. b), EHDS.

[115] Parere 1/15 della Corte, punto 32 (corsivo aggiunto).

[116] Questi aspetti verranno approfonditi nella sezione 3.1.1 del capitolo 3.

di disposizioni dello EHDS che mirano ad assicurare la libera circolazione dei dati sanitari personali nell'Unione. Un esempio è rappresentato dalle norme che consentono alle persone fisiche di trasmettere i propri dati sanitari elettronici, o una loro copia, a professionisti sanitari stabiliti in uno Stato membro diverso da quello di affiliazione, tramite l'utilizzo del formato europeo di scambio delle cartelle cliniche elettroniche nel contesto della piattaforma per l'uso primario (MyHealth@EU) [117].

In linea con l'approccio valoriale dell'Unione nella regolamentazione del mondo digitale [118], tramite il ricorso all'art. 16, par. 2, TFUE, il legislatore europeo punta a favorire l'innovazione, senza tuttavia compromettere il rispetto dei valori europei, compresi i diritti fondamentali, tra cui il diritto alla protezione dei dati personali [119]. Quest'ultimo, sebbene abbia acquisito un carattere sovraordinato rispetto ad altri diritti costituzionalmente garantiti a livello europeo [120], non è l'unico diritto fondamentale che disposizioni fondate sull'art. 16, par. 2, TFUE possono tutelare. La sua natura non assoluta consente infatti di bilanciarlo con altri diritti fondamentali, come il diritto alla salute [121] e la libertà dei cittadini di circolare nell'Unione nell'atto di ricevere servizi di assistenza sanitaria in uno Stato membro diverso da quello di affiliazione [122].

Per quanto riguarda poi l'art. 114 TFUE, il suo utilizzo come fondamento normativo dello EHDS è giustificato dalla necessità di rafforzare le libertà del mercato interno e, in particolare, la libera circolazione delle cartelle cliniche elettroniche e dei dati sanitari elettronici non personali in esse contenuti. Ad esempio, l'introduzione di un sistema di autocertificazione obbligatoria per

---

[117] Artt. 15, 7 e 23 EHDS.

[118] C. AMALFITANO, F. FERRI, *op. cit.*, 2023.

[119] Art. 8 Carta. Per un esame critico di tale disposizione, si rimanda alla sezione 4.2 del capitolo 2.

[120] Cfr. B. PETKOVA, *Privacy as Europe's First Amendment*, in *Eur. Law J.*, 2019, vol. 25, n. 2, pp. 140-154: che definisce il diritto alla protezione dei dati personali come "*Europe's first amendment*".

[121] Art. 35 della Carta, che viene richiamato nel documento di lavoro dei servizi della Commissione sulla valutazione d'impatto che accompagna il documento regolamento del Parlamento europeo e del Consiglio sullo Spazio europeo dei dati sanitari, SWD(2022) 131 final, parte 2/4, del 3 maggio 2022, p. 53.

[122] Art. 3, par. 2, TUE; art. 21 TFUE e art. 45 della Carta. Nella direttiva 2011/24/UE, così come nello EHDS, non vi è alcun riferimento alle norme sulla cittadinanza, probabilmente perché "l'accesso a cure mediche necessarie in altri Stati membri continua a configurarsi come un dovere per gli Stati membri anziché come diritto soggettivo ad ottenere cure tempestive e di qualità nell'Unione" (G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, p. 198). Si noti tuttavia come, durante la pandemia, l'art. 21, par. 2, TFUE ha rappresentato la base giuridica del regolamento (UE) 2021/953 del 14 giugno 2021 sul certificato COVID digitale dell'UE.

coloro che immettono le cartelle cliniche elettroniche nel mercato interno [123] dovrebbe evitare che iniziative nazionali provochino una frammentazione del mercato tale da generare, tra le altre cose, costi per le imprese tenute a conformarsi a regimi di certificazione differenti (armonizzazione preventiva).

Il legame con il mercato interno risulta meno evidente con riferimento alla libera circolazione dei pazienti nell'Unione [124]. Come osservato in dottrina, è difficile immaginare che consentire ai pazienti di portare con sé i propri dati sanitari o permettere ai professionisti sanitari di accedere ai dati personali dei pazienti e scambiarseli in formato elettronico attraverso l'infrastruttura MyHealth@EU [125] possa effettivamente aumentare la mobilità dei pazienti nell'Unione [126], i quali da tempo hanno dimostrato una scarsa propensione a spostarsi da uno Stato all'altro per ricevere cure sanitarie [127]. Al contrario, i principali effetti positivi derivanti dall'armonizzazione delle regole sull'uso primario si manifesteranno presumibilmente nelle situazioni interne, piuttosto che in quelle caratterizzate da elementi transfrontalieri [128].

Al di là di quest'ultime considerazioni, la presente analisi non intende mettere in discussione che lo EHDS persegua obiettivi riconducibili, da un lato, alla protezione degli individui rispetto al trattamento dei loro dati e, dall'altro, al rafforzamento del mercato interno [129], né che l'art. 114 TFUE possa

---

[123] Capo III EHDS.

[124] Considerando 7 EHDS.

[125] Capo II EHDS.

[126] In questo senso, di J. VAN DE GRONDEN, M. VEENBRINK, *EHDS and Free Movement of Patients: What EU Intervention is Needed?*, in *Eur. J. Health Law*, 2024, pp. 270-271.

[127] Cfr. relazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, COM(2022) 210 final, del 12 maggio 2022.

[128] J.S. MARCUS et al., *The European Health Data Space*, Publication for the Committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2022, p. 31.

[129] Soprattutto se si considera il mercato nella sua accezione quale "ambito al cui interno trovano […] pieno riconoscimento anche valori e interessi di matrice non commerciale" (F. COSTAMAGNA, *op. cit*., 2011, p. 213). Sul collegamento tra mercato interno e il perseguimento di obiettivi di natura non economica, cfr. B. DE WITTE, *op. cit*., 2012, p. 37 ss.; T.M. MOSCHETTA, *op. cit*., 2018, p. 39 ss.; E. TREGGIANI, *La complessa vicenda dei diritti sociali fondamentali nell'Unione europea*, in *SIE*, 2014, n. 1, p. 9; S. WEATHERILL, *Law and Values in the European Union*, OUP, Oxford, 2016; P.C. DE SOUSA, *The European Fundamental Freedoms: A Contextual Approach*, OUP, Oxford, 2015; D. DAMJANOVIC, *The EU Market Rules as Social Market Rules: Why the EU Can Be a Social Market Economy*, in *CMLRev*., 2013, vol. 50, n. 6, p. 1685; M. KRAJEWSKY, *Providing Legal Clarity and Securing Policy Space for Public Services through a Legal Framework for Services of General Economic Interest: Squaring the Circle*, in *Eur. Public Law*, 2008, vol. 14, n. 3, p. 395; G. CAGGIANO, *La "filigrana del mercato" nello status di cittadino europeo*, in E. TRIGGIANI (a cura di), *Le nuove*

legittimamente fungere da base giuridica anche per l'adozione di misure in materia di sanità, purché funzionali all'instaurazione o al funzionamento del mercato interno. La sola presenza di finalità sanitarie, anche rilevanti, non è pertanto sufficiente, di per sé, a escludere il ricorso alla base giuridica di cui all'art. 114 TFUE.

Ciò che merita tuttavia di essere approfondito è se, alla luce del contenuto complessivo dello EHDS [130], la tutela e il miglioramento della salute umana restino un obiettivo meramente strumentale rispetto a quello del mercato interno, oppure assumano un peso tale da incidere sull'individuazione del corretto "centro di gravità" dell'atto. In altri termini, la questione non è se lo EHDS persegua anche obiettivi di tutela della salute – circostanza difficilmente contestabile [131] – bensì se tali obiettivi possano essere qualificati come esclusivamente accessori rispetto a quelli immeditati, secondo i criteri elaborati dalla giurisprudenza della Corte in materia di basi giuridiche.

Sotto questo profilo, diversi elementi inducono a ritenere che le finalità connesse all'attuazione del diritto alla salute e, più in generale, alla creazione di un'UES [132] non si esauriscano in una funzione di mero supporto alla libera circolazione, ma concorrano in modo significativo a definire la *ratio* complessiva dello EHDS.

In primo luogo, le disposizioni relative all'uso primario dei dati sanitari elettronici mirano esplicitamente a migliorare la qualità, la sicurezza e la continuità delle cure, anche al di là delle ipotesi di mobilità transfrontaliera dei pazienti. Sebbene tali misure possano costituire una precondizione per una più effettiva circolazione dei pazienti e dei servizi sanitari [133], i loro effetti principali appaiono destinati a manifestarsi soprattutto nei contesti interni, incidendo sull'organizzazione e sull'efficienza dei sistemi sanitari nazionali. Un analogo obiettivo di continuità nelle cure e di accesso ai trattamenti sanitari è perseguito anche attraverso le norme che regolano i sistemi di cartelle cliniche

---

frontiere della cittadinanza europea, Cacucci, Bari, 2011, p. 215; G. TESAURO, *Diritto dell'Unione europea*, Cedam, Padova, 2012, p. 396.

[130] Per una ricostruzione critica del contenuto dell'atto e, in particolare, delle norme relative all'uso primario e secondario dei dati sanitari elettronici, si rinvia all'esame svolto nel capitolo 2. L'ordine di trattazione risponde all'esigenza di delineare preliminarmente il quadro costituzionale di riferimento, entro il quale l'analisi sostanziale dell'atto può essere collocata e valutata in modo puntuale.

[131] In senso analogo, cfr. J. VAN DE GRONDEN, M. VEENBRINK, *op. cit.*, 2024, pp. 270-272. Come sottolineato dalla Commissione stessa nella motivazione allegata alla proposta dello EHDS, gli obiettivi perseguiti con tale atto sono di assicurare un elevato livello di protezione della salute degli individui e, contemporaneamente, di garantire il corretto funzionamento del mercato unico per i prodotti di sanità digitale, anche attraverso un utilizzo più efficace dei dati sanitari.

[132] Questo aspetto verrà ulteriormente approfondito nella sezione 4.1 del capitolo 2.

[133] Art. 3, par. 2, TUE e artt. 20, par. 2, lett. a) e 21, par. 1, TFUE.

elettroniche. L'introduzione di requisiti di interoperabilità e autocertificazione obbligatoria mira, infatti, a facilitare lo scambio dei dati sanitari e a incrementare l'efficienza complessiva dei sistemi di assistenza sanitaria.

In secondo luogo, le norme sull'uso secondario dei dati sanitari perseguono obiettivi di interesse generale (ad es. la ricerca scientifica, l'innovazione terapeutica, la prevenzione e la gestione delle emergenze sanitarie) che risultano solo indirettamente collegati al funzionamento del mercato interno. L'accesso e la valorizzazione dei dati sanitari, nel rispetto delle norme sulla protezione dei dati personali, sono infatti concepiti principalmente come strumenti per il miglioramento dello stato di salute della popolazione e per il rafforzamento delle capacità decisionali e operative delle autorità pubbliche, piuttosto che come misure direttamente volte alla rimozione di ostacoli agli scambi.

Infine, nell'ottica della costruzione di un'UES [134], lo EHDS si inserisce in una strategia più ampia di rafforzamento delle competenze e delle capacità operative di agenzie e organismi dell'Unione, come HERA, EMA e ECDC. Esso contribuisce, in particolare, alla gestione coordinata delle crisi sanitarie (ad es. nel contesto del sistema di allarme rapido e di reazione) e al perseguimento di obiettivi strategici dell'Unione in ambito sanitario, quali quelli delineati nella strategia farmaceutica per l'Europa [135] e nel piano sulla lotta contro il cancro [136]. Anche in questo caso, il nesso con il mercato interno appare mediato e funzionale a finalità di tutela della salute pubblica.

---

[134] Come affermato nella spiegazione allegata alla proposta della Commissione sullo EHDS, tale atto "sosterrà il lavoro dell'Autorità europea per la preparazione e la risposta alle emergenze sanitarie (HERA), la missione dell'UE dedicata al cancro nel piano europeo di lotta contro il cancro e la strategia farmaceutica per l'Europa. Lo spazio europeo dei dati sanitari creerà un contesto giuridico e tecnico che sosterrà lo sviluppo di medicinali e vaccini innovativi, nonché di dispositivi medici e di diagnosi in vitro. Ciò aiuterà a prevenire e rilevare le emergenze sanitarie e a rispondervi rapidamente. Inoltre, lo spazio europeo dei dati sanitari contribuirà a migliorare la comprensione, la prevenzione, l'individuazione precoce, la diagnosi, la cura e il monitoraggio del cancro, attraverso l'accesso sicuro a livello transfrontaliero nell'UE a dati sanitari di persone fisiche, compresi i dati relativi al cancro, e la condivisione sicura di tali dati tra prestatori di assistenza sanitaria. Fornendo un accesso sicuro a un'ampia gamma di dati sanitari elettronici, lo spazio europeo dei dati sanitari creerà pertanto nuove opportunità per la prevenzione delle malattie e la cura delle persone fisiche" (COM(2022) 197 final, pp. 4-5).

[135] https://health.ec.europa.eu/medicinal-products/pharmaceutical-strategy-europe_it. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia farmaceutica per l'Europa, COM(2020) 761 final, del 25 novembre 2020, con cui la Commissione ha espresso l'intenzione di riesaminare la normativa farmaceutica per migliorare la sicurezza dell'approvvigionamento e affrontare le carenze di medicinali in situazioni di emergenza.

[136] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union/cancer-plan-europe_it. Si veda, in particolare, la Comunicazione della Commissione al Parlamento europeo e al Consiglio, Piano europeo di lotta contro il cancro, COM(2021) 44 final, del 3 febbraio 2021, pp. 6-7.

Considerato il potenziale contributo dello EHDS all'attuazione del diritto alla salute e alla realizzazione dell'UES, può dunque essere sostenuto che l'art. 168 TFUE avrebbe dovuto costituire, almeno in combinato disposto con gli artt. 114 e 16, par. 2, TFUE [137], una base giuridica idonea per l'adozione di tale regolamento. La mancata inclusione dell'art. 168 TFUE solleva pertanto interrogativi non tanto sull'ammissibilità astratta della base giuridica prescelta, quanto sulla coerenza complessiva dello EHDS con l'equilibrio costituzionale delle competenze in materia di sanità, tenuto conto dei limiti che tale disposizione avrebbe comportato in termini di perimetro e intensità dell'intervento dell'Unione.

A questo proposito, nei documenti preparatori all'adozione dello EHDS, è la Commissione stessa a riconoscere, in una sorta di ammissione di sconfinamento o perlomeno di uso improprio delle basi giuridiche, che il ricorso all'art. 168 TFUE avrebbe consentito "*a more limited scope for Union intervention, which would not [have] allow[ed] to tackle the problems for which the proposal has been conceived (e.g. supporting control of patients over their health data by improving interoperability, allowing the digital health products and services to circulate freely within the EU and re-using health data)*" [138].

---

[137] Come noto, la previsione di molteplici basi giuridiche non è vietata dalla giurisprudenza della Corte. Se infatti l'azione dell'Unione è volta a perseguire diversi obiettivi tra i quali non esiste un rapporto gerarchico, è possibile fare riferimento a basi giuridiche differenti che non prevedono procedure legislative incompatibili e che non compromettono così l'equilibrio interistituzionale, soprattutto per quanto riguarda le prerogative del Parlamento europeo. Cfr. sentenze della Corte del 10 gennaio 2006, causa C-178/03, *Commissione c. Parlamento e Consiglio*, ECLI:EU:C:2006:4, punto 57; del 10 dicembre 2002, causa C-491/01, *British American Tobacco*, ECLI:EU:C:2002:741, punti 103-111; dell'11 giugno 1991, causa C-300/89, *Commissione c. Consiglio*, ECLI:EU:C:1991:244, punti 18-20. Al contrario, qualora sia possibile individuare una gerarchia tra gli obiettivi perseguiti dall'atto in questione secondo il c.d. test del "centro di gravità", la Corte consente di fondare tale atto sulla base giuridica richiesta dallo scopo o dalla componente preponderante. Cfr. sentenza *Repubblica ceca c. Parlamento e Consiglio*, punto 31; sentenze della Corte del 29 aprile 2004, causa C-338/01, *Commissione c. Consiglio*, ECLI:EU:C:2004:253, punto 55; del 12 dicembre 2002, causa C-281/01, *Commissione c. Consiglio*, ECLI:EU:C:2002:761, punto 34; del 30 gennaio 2001, causa C-36/98, *Spagna c. Consiglio*, ECLI:EU:C:2001:64, punto 59; del 25 febbraio 1999, cause riunite C-164 e 165/97, *Parlamento c. Consiglio*, ECLI:EU:C:1999:99, punto 16; del 12 novembre 1996, causa C-84/94, *Regno Unito e Irlanda del Nord c. Consiglio*, ECLI:EU:C:1996:431, punto 22; del 9 ottobre 1995, causa C-426/93, *Repubblica federale della Germania c. Consiglio*, ECLI:EU:C:1995:367, punto 33; del 28 giugno 1994, causa C-187/93, *Parlamento c. Consiglio*, ECLI:EU:C:1994:265, punti 23-26; del 23 febbraio 1988, causa C-68/86, *Regno Unito e Irlanda del Nord c. Consiglio*, ECLI:EU:C:1988:85, punti 14-16.

[138] SWD(2022) 131 final, parte 1/4, p. 28. Tali chiarimenti sono stati forniti dalla Commissione, in risposta alle obiezioni sollevate dal Comitato per il controllo normativo che aveva chiesto di spiegare "*why Article 168(1) of the TFEU is not the main legal basis given that the*

3.2. Il ricorso agli artt. 114 e 16 TFUE per un quadro normativo armonizzato

Da quanto sopra, emerge chiaramente che la base giuridica dello EHDS è sostanzialmente il risultato di una scelta strategica dettata da esigenze di efficienza normativa. I vincoli imposti dall'art. 168 TFUE all'azione dell'Unione in questo settore non avrebbero permesso di garantire "un elevato livello di protezione della salute umana" [139]. Pertanto, il legislatore europeo, generando un vero e proprio cortocircuito costituzionale-legislativo, ha preferito optare per una base giuridica "forte" che giustificasse un intervento più incisivo da parte dell'Unione.

Come noto, infatti, in materia di mercato interno, l'Unione gode di una competenza concorrente che le consente di armonizzare le discipline fissate a livello nazionale [140]. In particolare, l'art. 114, par. 1, TFUE attribuisce al Parlamento europeo e al Consiglio la facoltà di adottare misure relative al ravvicinamento delle disposizioni legislative, regolamentari e amministrative nazionali per la creazione e il funzionamento di un mercato unico [141].

---

proposal's core objective is better healthcare for citizens, while Article 114 relates to establishment of a single market for digital health data that is more focused on the potential commercial exploitation of this data". Per via di queste osservazioni, la Commissione, oltre a specificare ulteriormente la scelta della duplice base giuridica (SWD(2022) 131 final, parte 2/4, sottosezione 3.1), ha eliminato ogni riferimento alla sanità pubblica tra gli obiettivi della proposta (SWD(2022) 131 final, parte 2/4, capitolo 4). In questa occasione, la Commissione ha anche sottolineato che la scelta di non utilizzare l'art. 168 TFUE come base giuridica del regolamento è dovuta al fatto che lo EHDS mira a promuovere l'accesso a dati di qualità sia per l'uso primario sia per quello secondario, lasciando agli utilizzatori la facoltà di servirsi degli stessi per migliorare i risultati sanitari. Di conseguenza, l'effetto dello EHDS sui risultati sanitari "*is a secondary effect of the main aims of the initiative*" (SWD(2022) 131 final, parte 1/4, p. 28).

[139] Art. 35 della Carta e art. 168, par. 1, TFUE.

[140] Sui tipi di armonizzazione, si rinvia a J. SNELL, *The Internal Market and the Philosophies of the European Union*, in C. BARNARD, S. PEERS, *European Union Law*, OUP, Oxford, 2020, p. 361 ss.; L. AZOULAI, *The Complex Weave of Harmonization*, in D. CHALMERS, A. ARNULL (eds.), *The Oxford Handbook of European Union Law*, OUP, Oxford, 2015; M. DOUGAN, *Minimum Harmonization and the Internal Market*, in *CMLRev*., 2000, vol. 37, p. 853; M. KLAMERT, *What We Talk About When We Talk About Harmonization*, in *Camb. Yearb. Eur. Leg. Stud*., 2015, vol. 17, p. 360; I. MALETIC, *The Law and Policy of Harmonization in Europe's Internal Market*, Edward Elgar, Cheltenham, 2013; S. WEATHERILL, *op. cit*., 2011, p. 827; S. WEATHERILL, *Maximum versus Minimum Harmonization: Choosing between Unity and Diversity in the Search for the Soul of the Internal Market*, in N.N. SHUIBHNE, L.W. GORMLEY (eds.), *From Single Market to Economic Union: Essays in Memory of John A. Usher*, OUP, Oxford, 2012, pp. 175-200.

[141] Per un commento all'art. 114 TFUE, cfr. M. KELLERBAUER, *Articles 114-118*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *The EU Treaties and the Charter of*

Inoltre, l'art. 16, par. 2, TFUE – introdotto con il Trattato di Lisbona – riconosce al legislatore dell'Unione il potere di adottare misure relative alla tutela delle persone fisiche rispetto al trattamento dei loro dati personali e alla libera circolazione degli stessi [142]. Sebbene la protezione e la libera circolazione dei dati personali non siano espressamente menzionate nell'elenco di cui all'art. 4, par. 2, TFUE, la dottrina è unanime nel ritenere che l'Unione abbia una competenza concorrente in questo settore [143]. Alcuni ritengono addirittura che, in questo ambito, l'Unione abbia una competenza esclusiva che è tale non per natura, ma per esercizio, dal momento che la protezione dei dati personali è disciplinata in modo quasi del tutto esaustivo dal GDPR [144].

Secondo uno schema tipico dell'approccio neo-funzionalista, quindi, la stretta interazione tra il mercato unico digitale e la protezione dei dati personali permette al legislatore europeo di raggiungere, con lo EHDS, una più ampia e profonda integrazione anche nel settore della salute (digitale). In particolare, l'utilizzo di una base giuridica "forte" consente di realizzare obiettivi che in passato non sono stati raggiunti con atti basati su un fondamento normativo che potremmo definire, all'opposto, come "debole".

Basti pensare alla limitata efficacia della direttiva 2011/24/UE in materia di sanità elettronica [145]. La natura volontaria di alcune delle sue disposizioni [146]

Fundamental Rights: A Commentary, OUP, Oxford, 2019, p. 1236 ss.; D. WYATT, *Community Competence to Regulate the Internal Market*, in M. DOUGAN, S. CURRIE (eds.), *50 Years of the European Treaties: Looking Back and Thinking Forward*, Hart Publishing, Oxford, 2009; I. MALETIĆ, *Derogations from the Regulation of Free Movement: Article 114 TFUE*, in P. KOUTRAKOS, J. SNELL (eds.), *Research Handbook on the Law of the EU's Internal Market*, Edward Elgar, Cheltenham, 2017, pp. 384-398; J. SNELL, *op. cit*., 2020, p. 355.

[142] Sull'art. 16 TFUE, cfr. M. KLAMERT, *Articles 15-16*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019, p. 405 ss.; F. POCAR, M.C. BARUFFI, A. ADINOLFI, *Commentario breve ai Trattati dell'Unione europea*, Cedam, Assago, 2014, p. 189 ss.

[143] G. ZANFRIN-FORTUNA, *Article 16 TFEU – Commentary*, in H-J.BLANKE, S. MANGIAMELI (eds.), *The Treaty on the Functioning of the European Union. A Commentary*, Springer, Berlin, 2021, p. 4; H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, Springer, Cham, 2016, p. 72.

[144] L. DALLA CORTE, *On Proportionality in the Data Protection Jurisprudence of the CJEU*, in *Int. Data Priv. Law*, 2022, vol. 12, n. 4, p. 264.

[145] Per un'analisi approfondita degli aspetti della direttiva 2011/24/UE relativi all'assistenza sanitaria online e alla valutazione delle tecnologie sanitarie, cfr. G. DI FEDERICO, S. NEGRI, *op. cit*., 2019, p. 221 ss.

[146] In particolare, vale la pena ricordare che la direttiva 2011/24/UE prevede, su base volontaria, la creazione della Rete di assistenza sanitaria online, costituita da "autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri" (art. 14, par. 1), anche per permettere la condivisione dei dati sanitari nell'assistenza sanitaria transfrontaliera. Per fare ciò, la Rete può adottare linee guida sui dati da inserire nei fascicoli dei pazienti, definire metodi di scambio delle informazioni mediche per finalità relative alla prevenzione, cura e ricerca (art. 14, par. 2, lett. b)), nonché stabilire "misure comuni di identificazione e

ha impedito di assicurare alle persone fisiche il controllo sui propri dati sanitari elettronici, sia a livello nazionale che transfrontaliero, e di promuovere l'uso di tali dati per scopi specifici (ad es. assistenza sanitaria e ricerca scientifica). Per raggiungere questi risultati, sarebbe stata necessaria un'armonizzazione [147] che, tuttavia, non è stata possibile a causa della scelta di fondare la direttiva 2011/24/UE non solo sull'art. 114 TFUE, ma anche sull'art. 168 TFUE.

A questo proposito, vale la pena ricordare che, durante l'iter di adozione dell'atto [148], gli Stati membri, rappresentati in seno al Consiglio, hanno esercitato forti pressioni affinché la proposta della Commissione venisse modificata per includere, oltre all'art. 114 TFUE, anche l'art. 168 TFUE. In ragione dell'interpretazione estensiva offerta dalla Corte rispetto al concetto di mercato interno [149], il Consiglio ha riconosciuto la pertinenza dell'art. 114 TFUE come base giuridica per le disposizioni della direttiva direttamente connesse al mercato interno [150]. Tuttavia, allo scopo di valorizzare la dimensione sociale dell'atto, il Consiglio ha ritenuto che non si potesse prescindere dall'art.

---

autenticazione", senza cui lo scambio dei dati nell'assistenza sanitaria transfrontaliera sarebbe limitata (art. 14, par. 2, lett. b). Vedi anche la decisione di esecuzione 2011/890/UE della Commissione del 22 dicembre 2011). Dal 2013, la Rete è inoltre responsabile della gestione della piattaforma *eHealth Digital Service Infrastructure* (eHDSI), finanziata dal Meccanismo per collegare l'Europa, con lo scopo di assicurare la portabilità dei dati sanitari contenuti nelle prescrizioni elettroniche e nei fascicoli elettronici sintetici (*patient summary*). Per rendere effettiva la circolazione delle prescrizioni, la Rete ha adottato, nel novembre 2014 e 2016, apposite linee guida sulle prescrizioni elettroniche relative ai prodotti farmaceutici (cfr. *Guideline on ePrescriptions Dataset for Electronic Exchange under Cross-Border Directive 2011/24/UE*, 2014 e *Guideline on the Electronic Exchange of Health Data under Cross-Border Directive 2011/24/UE*, 2016). Quanto poi ai fascicoli sanitari elettronici, la Rete ha approvato, rispettivamente nel novembre 2013 e 2016, orientamenti sull'elenco non esaustivo di dati sanitari da includere nei fascicoli, distinguendo tra dati amministrativi e dati clinici (cfr. *Guideline on Minimum/Nonexhaustive Patient Summary Dataset for Electronic Exchange in Accordance with the Cross-Border Directive 2011/24/UE*, 2013, aggiornate nel 2016).

[147] SWD(2022) 131 final, parte 1/4, e DG SANTE, *Study Supporting the Impact Assessment of Policy Options for an EU Initiative on a European Health Data Space*, 2022.

[148] Sul lungo e tortuoso iter legislativo che ha portato all'adozione della direttiva, si veda G. DI FEDERICO, *op. cit*., 2012, pp. 683-704; M. INGLESE, *op. cit*., 2012, pp. 109-138; M. PEETERS, *op. cit*., 2012, pp. 29-60; S. WOLF, *The Proposed Patients' Rights Directive and the Reform of (Cross-Border) Healthcare in the European Union*, in *Leg. Issues Econ. Integr.*, 2009, vol. 35, n. 2, pp. 109-131; S. DE LA ROSA, *The Directive on Cross-Border Healthcare or the Art of Codifying Complex Case Law*, in *CMLRev*., 2012, vol. 49, n. 1, pp. 15-46.

[149] Cfr. T. HORSLEY, *op. cit*., 2022, p. 209: "*Had the Court adopted a stricter, functional approach to the scope of its competences as direct policymaker, the Union legislature may not have succeeded in using (or even attempted to use) the Treaties' internal market provision as a legal basis for legislative policymaking in the area of cross-border healthcare*".

[150] Si pensi, ad esempio, alle norme contenute nei Capi II e III della direttiva 2011/24/UE sulla possibilità di chiedere il rimborso delle spese affrontate per ricevere trattamenti sanitari nello Stato membro di cura.

168 TFUE quale fondamento costituzionale per le disposizioni volte a perseguire obiettivi extra-economici con implicazioni significative riguardo all'erogazione di servizi sanitari e, in generale, alle politiche sanitarie nazionali [151].

Questa scelta del fondamento giuridico per la direttiva è stata quindi una soluzione di compromesso tra il perseguimento dell'obiettivo trasversale di cui all'art. 9 TFUE e il rispetto dell'autonomia regolamentare degli Stati membri ai sensi dell'art. 168, par. 7, TFUE, per evitare "qualsiasi armonizzazione e indesiderate derive mercantilistiche" [152].

Analoghe considerazioni hanno orientato la scelta della base giuridica per il regolamento (UE) 2021/2282 sulla valutazione delle tecnologie sanitarie (regolamento HTA) che, da un lato, stabilisce procedure e norme comuni per lo svolgimento di attività congiunte in materia di valutazione delle tecnologie e, dall'altro, sostiene gli Stati nella cooperazione su alcuni aspetti delle valutazioni [153]. Abbandonando l'iniziale proposta di fondare il regolamento HTA unicamente sull'art. 114 TFUE [154], poiché ciò avrebbe confermato "un approccio prevalentemente mercantilistico nel settore dell'assistenza sanitaria transfrontaliera" [155], il testo finale vede una duplice base giuridica, composta dagli artt. 114 e 168 TFUE.

---

[151] In particolare, secondo il Consiglio, l'art. 114 TFUE costituiva la base giuridica più opportuna per le norme che presentano un legame immediato con il mercato interno (ad es. quelle relative al rimborso delle spese per l'assistenza sanitaria ricevuta all'estero). L'art. 168 TFUE, invece, doveva rappresentare il fondamento normativo più adeguato per le disposizioni volte a realizzare obiettivi ulteriori rispetto al completamento del mercato interno, ossia la cooperazione tra Stati membri in materia di assistenza sanitaria con disposizioni che incidono sulla modalità di organizzazione e fornitura dei servizi sanitari e sulle scelte di politica sanitaria nazionale (ad es. le norme sulla sicurezza e la qualità dei trattamenti e sulla creazione di reti di riferimento europee). Diversamente, sia la Commissione sia il Parlamento europeo si opposero all'inserimento dell'art. 168 TFUE accanto all'art. 114 TFUE. Cfr. F. COSTAMAGNA, *op. cit*., 2011, p. 210 ss.

[152] G. DI FEDERICO, S. NEGRI, *op. cit*., 2019, p. 198.

[153] Regolamento (UE) 2021/2282 del Parlamento europeo e del Consiglio del 15 dicembre 2021 relativo alla valutazione delle tecnologie sanitarie e che modifica la direttiva 2011/24/UE. A tale riguardo si noti, tuttavia, che la proposta della Commissione era fondata unicamente sull'art. 114 TFUE. Tale scelta rifletteva l'intento di rispondere a "esigenze di efficienza e sostenibilità": da un lato, imponendo la partecipazione di tutti gli Stati membri e prevenendo sovrapposizioni operative a livello nazionale, con conseguenti risparmi in termini di costi; dall'altro lato, conferendo alla cooperazione amministrativa transfrontaliera un carattere stabile sia sotto il profilo della partecipazione che del finanziamento (G. DI FEDERICO, S. NEGRI, *op. cit*., 2019, p. 234).

[154] Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla valutazione delle tecnologie sanitarie, che modifica la direttiva 2011/24/UE, COM(2018) 51 final, del 31 gennaio 2018.

[155] G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, p. 238.

In questo modo, anziché affidare la tutela della sanità pubblica alla clausola dell'art. 114, par. 3, TFUE, il legislatore ha posto esplicitamente tale obiettivo al centro del regolamento, il quale "mira a conseguire un elevato livello di protezione della salute dei pazienti e degli utilizzatori garantendo al contempo il buon funzionamento del mercato interno per quanto riguarda i medicinali, i dispositivi medici e i dispositivi medico-diagnostici in vitro" [156].

Con lo EHDS, osservazioni come quelle appena menzionate, volte a mitigare la dimensione mercantilistica dell'integrazione europea e a salvaguardare l'autonomia regolamentare degli Stati nel rispetto del sistema di ripartizione delle competenze, sembrano essere state secondarie rispetto alle motivazioni legate all'efficienza normativa. Al fine di raggiungere gli obiettivi prefissati, il legislatore europeo ha optato per un uso creativo o poco ortodosso delle sue competenze anziché conformarsi rigorosamente al principio di attribuzione [157]. Da qui deriva, come si diceva, la scelta di non inserire l'art. 168 TFUE tra le disposizioni di diritto primario che rappresentano la base giuridica dello EHDS. Una scelta diversa avrebbe limitato l'intervento dell'Unione alla sola promozione della cooperazione tra gli Stati membri, escludendo qualsiasi possibilità di armonizzazione normativa.

Come anticipato in apertura, infatti, in materia di tutela e miglioramento della salute umana [158], l'Unione dispone di una competenza di tipo complementare [159]. Di conseguenza, gli atti giuridici vincolanti adottati in questo

---

[156] Considerando 11 regolamento HTA.

[157] Per una lettura critica del fondamento giuridico dello EHDS e, in particolare, del ricorso all'art. 114 TFUE, si rimanda all'analisi di J. VAN DE GRONDEN, M. VEENBRINK, *op. cit.*, 2024, pp. 249-284.

[158] Art. 168 TFUE. Cfr. S. GARBEN, *Article 168 TFEU*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019, p. 1448; M. MARLETTA, *Commento all'art. 168 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Giuffrè, Milano, 2014; M. MIGLIAZZA, *Art. 168. Sanità pubblica*, in F. POCAR, M.C. BARUFFI, A. ADINOLFI, *op. cit*., 2014, p. 1039 ss.; T. HERVEY, *Community and National Competence in Health After Tobacco Advertising*, in *CMLRev*., 2011, vol. 38, n. 6, pp. 1421-1461.

[159] Art. 6, lett. a), TFUE. Al contrario, secondo quanto disposto dall'art. 4, par. 2, lett. k), TFUE, l'Unione gode di una competenza concorrente con riferimento a "problemi comuni di sicurezza in materia di sanità pubblica". Per una precisa disamina delle competenze dell'Unione in ambito sanitario, cfr. G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, p. 173 ss.; G. DI FEDERICO, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in E. AL MUREDEN, C. BOTTARI (eds.), *La salute del futuro: prospettive e nuove sfide del diritto sanitario*, Bononia University Press, Bologna, 2020, pp. 18-20; D.G. RINOLDI, *Cercando Itaca: spazio europeo della salute, Next Generation EU e prospettive di approfondimento dell'integrazione continentale*, in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Giappichelli, Torino, 2023, pp. 14-16; T. CLEMENS, K. MICHELSEN, H. BRAND, *op. cit*., 2014, p. 49; F. BESTAGNO, *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in *SIE*, 2017, vol. 2, p. 317.

settore non possono portare a un'armonizzazione delle disposizioni legislative e regolamentari degli Stati membri [160]. L'azione dell'Unione deve piuttosto limitarsi a sostenere, coordinare e completare le politiche nazionali [161], promuovendo, ad esempio, la cooperazione e il coordinamento tra gli Stati membri per migliorare la complementarità dei loro servizi sanitari nelle regioni di frontiera attraverso l'elaborazione di orientamenti e indicatori e lo scambio di buone pratiche [162].

Le uniche eccezioni a tale divieto di armonizzazione si riferiscono alle sole misure con cui vengono stabiliti standard di qualità applicabili agli organi, alle sostanze di origine umana, al sangue e agli emoderivati [163], ai medicinali e dispositivi medici [164], nonché alle misure adottate nei settori veterinario e fitosanitario [165].

Al contrario, sono di competenza nazionale ai sensi dell'art. 168, par. 7, TFUE – è bene ribadirlo – la definizione della politica sanitaria, l'organizzazione e la fornitura di servizi sanitari e di assistenza medica, nonché la donazione e l'impiego medico di organi e sangue [166]. Tali prerogative sono riconosciute anche dall'art. 35 della Carta, che subordina l'esercizio del diritto di ogni individuo ad accedere alla prevenzione sanitaria e a ottenere cure mediche al rispetto delle "condizioni stabilite dalle legislazioni e prassi nazionali" [167].

---

[160] Art. 2, par. 5, TFUE. In materia di sanità pubblica, tale divieto viene richiamato in modo esplicito dall'art. 168, par. 5, TFUE.

[161] Artt. 2, par. 5 e 6, TFUE.

[162] Art. 168, par. 2, TFUE.

[163] Art. 168, par. 4, lett. a), TFUE. Come ricordato in precedenza, le misure che si fondano su questa disposizione non devono, ai sensi dell'art. 168, par. 7, TFUE pregiudicare "le disposizioni nazionali sulla donazione e l'impiego medico di organi e sangue". Sulla base di tale norma è stato possibile proporre, ad esempio, il regolamento sui parametri di qualità e sicurezza per le sostanze di origine umana destinate all'applicazione sugli esseri umani, COM(2022) 338 final, del 14 luglio 2022.

[164] Art. 168, par. 4, lett. c), TFUE. Si veda altresì la dichiarazione n. 32 relativa all'art. 168, par. 4, lett. c), TFUE in cui si afferma che l'adozione di misure basate su tale fondamento giuridico deve avvenire nei casi in cui le "norme nazionali aventi un impatto sul mercato interno impedirebbero altrimenti la realizzazione di un elevato livello di protezione umana". Tramite l'uso congiunto degli artt. 114 e 168, par. 4, lett. c), TFUE è stato, ad esempio, possibile adottare il regolamento sulla sperimentazione clinica (regolamento (UE) 536/2014) e il regolamento sui dispositivi medici (regolamento (UE) 2017/745).

[165] Art. 168, par. 4, lett. b), TFUE.

[166] Sull'esclusività della competenza degli Stati ad organizzare i propri sistemi previdenziali, si veda il costante orientamento della Corte nelle sentenze *Smits e Peerbooms*, punto 44; *Decker e Kohll*; sentenze del 17 giugno 1997, causa C-70/95, *Sodemare e a*., ECLI:EU:C:1997:301, punto 27; del 7 febbraio 1984, causa C-238/82, *Duphar e a*., ECLI:EU:C:1984:45, punto 16.

[167] Per un commento sull'art. 35 della Carta, cfr. G. DI FEDERICO, *Art. 35*, in R. MASTROIANNI et al. (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè,

Alla luce di tali limiti costituzionali, la scelta della Commissione è stata quella di porre l'accento sul rapporto tra lo EHDS e il mercato unico digitale [168], dove non solo i prodotti di sanità digitale possono circolare liberamente, ma anche i dati sanitari possono essere utilizzati e condivisi per finalità di cura o altre finalità di interesse generale nel rispetto delle norme sulla protezione dei dati personali, anziché sul legame tra lo EHDS e la tutela della salute nella prospettiva della creazione di un'UES. Come già più volte evidenziato, questa decisione è funzionale a un intervento maggiormente incisivo dell'Unione in questa materia "sensibile".

Nella medesima direzione si colloca la decisione sulla tipologia di atto adottato: non una direttiva, bensì un regolamento [169]. Poiché né l'art. 114 TFUE né l'art. 16, par. 2, TFUE impongono l'adozione di una specifica tipologia di strumento normativo, le istituzioni hanno la facoltà di scegliere il tipo di atto che meglio risponde agli obiettivi prefissati. Questa scelta dovrebbe comunque rispettare il principio di proporzionalità, che richiede che lo strumento normativo selezionato non solo sia idoneo a realizzare gli obiettivi prefissati, ma anche non vada oltre a quanto necessario per raggiungerli [170].

Come si avrà modo di approfondire in seguito, considerato il potenziale impatto dello EHDS sugli ordinamenti nazionali, sarebbe forse stato preferibile optare per una direttiva, limitando così l'intervento dell'Unione al ravvicinamento e all'armonizzazione delle legislazioni nazionali. La scelta del legislatore, tuttavia, risponde a una precisa logica: sfruttare la diretta applicabilità dei regolamenti e la vincolatività di tutti i loro elementi per ridurre il

---

Milano, 2017, pp. 664-679; T. HERVEY, J. MCHALE, *The Right to Health Care*, in S. PEERS et al. (eds.), *op. cit*., 2022, p. 1007 ss.; A. LUCARELLI, *Art. 35 Protezione della salute*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (eds.), *L'Europa dei diritti. Commento alla carta dei diritti fondamentali dell'Unione europea*, Il Mulino, Bologna, 2001, pp. 245-251; T. LOCK, *Articles 35-38*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019, p. 2195 ss.; F. POCAR, M.C. BARUFFI, A. ADINOLFI, *op. cit*., 2014, p. 1751; T. HERVEY, J. MCHALE, *Rights: Health Rights as Human Rights, in European Union Health Law: Themes and Implications*, CUP, Cambridge, 2015; G. STROZZI, *Il sistema integrato di tutela dei diritti fondamentali dopo Lisbona: attualità e prospettive*, in L.F. PACE (a cura di), *op. cit*., 2012, p. 36; B. TOEBES, *Right to Health and Health Care*, in D.P. FORSYTHE, *Encyclopaedia of Human Rights*, OUP, Oxford, 2009, p. 365.

[168] Considerando 1 proposta EHDS (COM(2022) 197 final).

[169] Spiegazione allegata alla proposta della Commissione sullo EHDS, p. 8. Sulla tendenza a ricorrere allo strumento normativo del regolamento per la realizzazione del mercato unico digitale, cfr. M. INGLESE, *Il regolamento sull'intelligenza artificiale come atti per il completamento e il buon funzionamento del mercato interno?*, in *Quaderni AISDUE*, 2024, fasc. 2, pp. 8-10 e le considerazioni svolte nella sezione 2.1 del capitolo 2.

[170] Cfr. P. MORI, *Art. 296*, in A. TIZZANO (a cura di), *op. cit.*, 2014, p. 2309 e giurisprudenza ivi citata.

margine di discrezionalità degli Stati membri e prevenire, almeno in linea teorica, la creazione di sistemi normativi frammentati.

4. La conformità dello spazio europeo dei dati sanitari rispetto al quadro costituzionale esistente

A fronte delle potenzialità derivanti dal ricorso combinato degli artt. 114 e 16, par. 2, TFUE in termini di efficienza normativa, non si possono trascurare, in un'Unione che si professa essere un'Unione di diritto [171], i rischi relativi alla conformità di tale scelta rispetto all'attuale assetto delle competenze dell'Unione. La decisione di fondare un atto su queste basi giuridiche può, infatti, alimentare il fenomeno della "*competence creep*" potenzialmente in tutti i settori che sono interessati dal processo di digitalizzazione. In ambito sanitario, ad esempio, l'evoluzione tecnologica, nei modelli di erogazione dell'assistenza sanitaria e nella conduzione della ricerca scientifica, permette di stabilire un legame tra un settore tradizionalmente ritenuto "sensibile" e soggetto alla sovranità statale, e ambiti, come il mercato interno e la protezione dei dati personali, che legittimano un intervento normativo più penetrante da parte dell'Unione, ampliandone così il raggio d'azione.

Con riferimento allo EHDS, sono rinvenibili diverse disposizioni che, pur collocandosi formalmente in una dimensione di coordinamento, testimoniano la volontà del legislatore europeo di orientare l'azione degli Stati membri in ambiti che i Trattati tradizionalmente riconducono alle loro prerogative. È il caso, in particolare, delle norme relative all'istruzione e alla formazione [172], nonché di quelle concernenti profili etici della sanità digitale [173]. Tali disposizioni,

---

[171] Sentenze della Corte del 3 settembre 2008, cause riunite C-402/05 P e C-415/05 P, *Kadi*, ECLI:EU:C:2008:461, punto 281; del 25 luglio 2002, causa C-50/00 P, *Unión de Pequeños Agricultores*, ECLI:EU:C:2002:462, punto 38; del 23 aprile 1986, causa 294/83, *Les Verts*, ECLI:EU:C:1986:166, punto 23.

[172] Non occorre ricordare che questo settore, in linea di principio, non rientra tra le competenze dell'Unione. Cfr. sentenza della Corte del 21 giugno 1988, causa 197/1988, *Brown*, ECLI:EU:C:1988:323, punto 18. Più recentemente, v. sentenza della Corte del 7 settembre 2022, causa C-391/20, *Cilevičs*, ECLI:EU:C:2022:638, punti 58-59, commentata da G. DI FEDERICO, G. MARTINICO, *Official Languages, National Identities and the Protection of Minorities: A Complex Legal Puzzle: Court of Justice (Grand Chamber) 7 September 2022, Case C-391/20, Boriss Cilevičs et al., ECLI:EU:C:2022:638*, in *Eur. Const. Law Rev.*, 2023, vol. 19, n. 2, pp. 346-370.

[173] In tale ambito, l'azione dell'Unione si limita generalmente all'adozione di atti privi di vincolatività. Si pensi, ad esempio, ai pareri e alle dichiarazioni del Gruppo europeo sull'etica nella scienza e nelle nuove tecnologie (EGE). Organo indipendente e multidisciplinare,

considerate isolatamente, presentano un contenuto essenzialmente programmatico e accessorio: esse non definiscono in modo puntuale l'azione richiesta agli Stati membri, né introducono obblighi giuridici sufficientemente determinati da incidere, di per sé, sulla scelta della base giuridica dell'atto.

Cionondimeno, la presenza di tali norme nel testo dello EHDS non è priva di rilievo sistemico. Inserite in un atto fondato sugli artt. 114 e 16, par. 2, TFUE, esse contribuiscono infatti a delineare un quadro regolatorio nel quale l'Unione non si limita a perseguire obiettivi funzionali alla realizzazione del mercato interno o alla disciplina del trattamento dei dati personali, ma tende progressivamente a estendere la propria influenza anche su ulteriori dimensioni delle politiche sanitarie nazionali, quali la formazione degli operatori, la sensibilizzazione della società e la definizione di cornici etiche di riferimento.

Con specifico riguardo alla formazione digitale [174], lo EHDS prevede due disposizioni in virtù delle quali gli Stati membri sono chiamati a istituire

---

nominato dal Presidente della Commissione europea, l'EGE offre consulenza circa gli aspetti delle politiche e della legislazione della Commissione che sollevano questioni etiche relativamente allo sviluppo della scienza e delle nuove tecnologie. I suoi pareri hanno l'obiettivo di orientare le scelte del legislatore europeo e dei legislatori nazionali affinché questi possano adottare atti che consentano ai propri cittadini di beneficiare delle potenzialità delle nuove tecnologie nel quadro della tutela dei valori europei. Nonostante la natura consultiva del suo ruolo, l'EGE ha esercitato e continua a esercitare una certa influenza sull'attività legislativa delle istituzioni europee, tanto che in passato è stata contestata l'assenza di una base giuridica che consentisse di definire i limiti della sua azione, specialmente tenendo conto che la sua composizione vede un legame stretto con la Commissione e non, invece, con i comitati etici nazionali (H. BUSBY, T. HERVEY, A. MOHR, *Ethical EU Law? The Influence of the European Group on Ethics in Science and New Technologies*, in *Eur. Law Rev*., 2008, vol. 33, pp. 837-839). Di recente, l'EGE ha avuto un ruolo determinante nell'orientare i lavori del gruppo ad alto livello di IA e dell'alleanza europea per l'IA (EGE, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, 2018), nonché nel supportare la Commissione nell'elaborazione delle iniziative da proporre per la costruzione di un'UES con specifico riferimento al miglioramento della preparazione e della gestione delle pandemie (EGE, *Improving Pandemic Preparedness and Management – Lessons Learned and Ways Forward – Independent expert report*, 2020). Nella direzione di un maggiore coinvolgimento dell'Unione nell'affrontare questioni di tipo etico si pone la Risoluzione del Parlamento europeo del 20 ottobre 2020 in cui, tra le altre cose, viene chiesto alla Commissione, in conformità con l'art. 225 TFUE, di presentare una proposta di regolamento sui principi etici relativi allo sviluppo, alla diffusione e all'utilizzo dell'intelligenza artificiale, della robotica e delle tecnologie correlate, a norma dell'art. 114 TFUE. L'introduzione di norme etiche è stata sollecitata anche dal Consiglio europeo nella riunione straordinaria dell'1 e del 2 ottobre 2020, EUCO 13/20, 2020, p. 7.

[174] Nel 2021, la Commissione ha dedicato un'ampia sezione della sua Comunicazione, Bussola per il digitale 2030, agli obiettivi di incremento delle competenze digitali nell'Unione. Oltre a rinviare all'esigenza di raggiungere un livello di alfabetizzazione digitale di base, espressa nel Pilastro europeo dei diritti sociali, la Commissione ha pianificato la creazione di centri di ricerca avanzati in campo teorico e applicativo (cfr. COM(2021) 118 final, del 9 marzo 2021, pp. 4-5 e, ancor prima, v. COM(2020) 66 final, del 19 febbraio 2020, p. 6 e COM(2020) 67 final, del 19 febbraio 2020, p. 6). La promozione di un'istruzione e una

programmi formativi rivolti ai professionisti, agli *stakeholders* e alla società nel suo complesso, al fine di rafforzare la "*digital health literacy*" [175]. Tali previsioni, pur non imponendo standard uniformi né definendo i contenuti dell'offerta formativa, contribuiscono a orientare le politiche nazionali in un ambito che, ai sensi dei Trattati, rientra primariamente nella competenza degli Stati membri.

Analogamente, in relazione alle questioni etiche, il regolamento invita gli Stati membri a conformarsi ai principi etici applicabili alla sanità digitale nell'attuazione dello EHDS [176]. Esso prevede inoltre che gli organismi responsabili dell'accesso ai dati effettuino, qualora tali valutazioni non siano già state svolte dai comitati etici nazionali [177], un esame degli aspetti etici connessi ai trattamenti di dati per finalità di uso secondario (ad es. autonomia,

---

formazione digitali di elevata qualità rientra anche tra gli impegni assunti dall'Unione per assicurare il diritto di ogni persona di acquisire tutte le competenze digitali di base e avanzate (punto 4 della Dichiarazione sui principi e i diritti digitali, COM(2022) 28 final, del 26 gennaio 2022). Inoltre, nella citata Risoluzione del Parlamento europeo sulle proposte di modifiche ai Trattati (2022/2051(INL)), è stato proposto di inserire l'istruzione tra le competenze concorrenti dell'Unione (art. 4, lett. k) *quater,* TFUE), invitando il legislatore a definire obiettivi e norme comuni per un'istruzione che, tra le altre cose, promuova l'alfabetizzazione digitale (art. 165, par. 2, trattino 1).

[175] Artt. 83-84 EHDS. Sulla questione dell'alfabetizzazione digitale in sanità, v. K. SØRENSEN, *Brussels – We Have a Health Literacy Problem,* in *Eurohealth*, 2022, vol. 28, n. 3, pp. 53-55; WHO, *Digital Education for Building Health Workforce Capacity*, 2020; WHO Regional Office for Europe, *Health and Care Workforce in Europe: Time to Act*, 2022; OECD, *Empowering the Health Workforce Strategies to Make the Most of the Digital Revolution*, 2020.

[176] Considerando 24 EHDS. I principi europei dell'etica della sanità digitale, adottati all'unanimità dagli Stai membri, come pure dalla Norvegia e dall'Islanda nel quadro della rete *eHealth*, si sviluppano su quattro dimensioni che attingono direttamente alle basi della cultura europea: i) fondare la sanità digitale su valori umanistici; ii) permettere alle persone di disporre dei propri dati sanitari e di controllarli; iii) fare in modo che la sanità digitale sia accessibile a tutti; iv) attuare una sanità digitale eco-responsabile. Molti dei principi elaborati corrispondono a quelli presenti nelle Conclusioni del 2006 del Consiglio sui valori e principi comuni dei sistemi sanitari dell'Unione europea (principio di equo accesso alla salute), nel GDPR (ad es. '*human oversight*'/'*human-in-the-loop*') e nella Dichiarazione europea sui diritti e i principi digitali per il decennio digitale.

[177] Artt. 68, par. 1, lett. f), e 67, par. 2, lett. j), EHDS. Nel corso dell'iter legislativo, diversamente dal Parlamento che ha insistito per l'introduzione di specifiche in materia etica, il Consiglio non ha avanzato modifiche sostanziali riguardo ai profili etici connessi al trattamento dei dati sanitari. Un'unica proposta merita di essere segnalata: l'inclusione, tra le attività di uso secondario vietate, di quelle in contrasto con le norme etiche nazionali (art. 35, par. 1, lett. f), *general approach* del Consiglio del 6 dicembre 2023). Sono fatte salve, però, le norme etiche relative al consenso, al diritto di opporsi al trattamento dei dati personali e al diritto di opposizione, per le quali, in applicazione del principio generale del primato del diritto dell'Unione, il regolamento prevale sul diritto nazionale (considerando 41 *general approach* del Consiglio).

privacy, confidenzialità e consenso informato), avvalendosi di organismi etici competenti [178].

Rispetto agli esempi appena citati, un intento più marcato da parte dell'Unione di orientare l'azione degli Stati membri emerge dalla lettura delle disposizioni dello EHDS che affrontano, anche solo indirettamente, questioni concernenti la tutela e il miglioramento della salute umana [179]. Queste disposizioni risultano problematiche per almeno due ragioni. In primo luogo, esse devono confrontarsi con l'obbligo, sancito dai Trattati, di rispettare l'autonomia degli Stati membri nell'organizzazione e nel finanziamento dei propri sistemi di assistenza sanitaria [180]. In secondo luogo, esse si collocano in un settore nel quale vige un espresso – benché non assoluto – divieto di armonizzazione delle disposizioni legislative e regolamentari nazionali [181].

Alla luce di tali considerazioni, nelle pagine successive si intende sollevare alcuni rilievi critici in merito alla compatibilità dello EHDS con il quadro costituzionale esistente (sezioni 4.1 e 4.3), esaminando anche la reazione degli Stati membri durante il processo legislativo rispetto alla direzione impressa dall'Unione al processo di integrazione europea (sezioni 4.2 e 4.4).

4.1. Il rispetto dell'autonomia degli Stati nella definizione delle loro politiche sanitarie

Nonostante quanto prescritto dall'art. 168 TFUE, la riserva contenuta nel suo ultimo paragrafo sembra oramai da considerarsi come mera clausola di salvaguardia o di cessione mobile delle competenze. Fatto salvo, infatti, che

---

[178] Art. 55, par. 2, EHDS. Si noti come un impulso alla trattazione di profili etici nello EHDS proviene specialmente dalla presidenza francese che si è occupata inizialmente del dossier. Nella sua nota informativa per la sessione del Consiglio EPSCO (Salute) del 14 giugno 2022, viene infatti sottolineato che, al di là di pilastri fondamentali come la sicurezza e l'interoperabilità, una fiducia basata sull'etica rappresenta il "requisito indispensabile affinché i cittadini sostengano lo sviluppo della sanità digitale" (p. 6).

[179] In dottrina, è già stato rilevato come la sanità digitale rappresenta "un ulteriore banco di prova per l'influenza materiale che le politiche sovranazionali esercitano sui livelli interni di governo e sulle modalità di interazione degli organi che ne compongono i circuiti rappresentativi" (R. MICCÙ, *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in *federalismi.it*, 2021, p. 2). Con specifico riferimento all'impronta sovranazionale nella fase di applicazione del diritto dell'Unione, si consenta il rinvio a A. FIORENTINI, *Alla ricerca di un punto di equilibrio tra autonomia istituzionale ed effettività del diritto per le forme di integrazione amministrativa nel settore digitale*, in *Quaderni AISDUE, Sezione "Atti convegni AISDUE"*, 2023, n. 30, pp. 652-673.

[180] Art. 168, par. 7, TFUE.

[181] Art. 2, par. 5, TFUE.

non vi sia una minoranza di blocco in seno al Consiglio [182], difficilmente tale disposizione può rappresentare un ostacolo all'azione dell'Unione. Al contrario, la sua presenza nei Trattati sembra avere come unico effetto [183] quello di vietare all'Unione di interferire nella scelta degli Stati membri sul modello organizzativo dei propri sistemi sanitari nazionali [184], nonché di obbligare il legislatore europeo a inserire negli atti di diritto derivato pertinenti formule generiche sul rispetto delle prerogative nazionali in questo settore.

Tali formule costellano il testo dello EHDS. Il legislatore europeo ribadisce a più riprese che il quadro normativo proposto non va in alcun modo a intaccare le prerogative degli Stati nella definizione della loro politica sanitaria, comprese le decisioni sui servizi che forniscono e rimborsano [185]. Allo stesso tempo, però, viene specificato che, ad esempio, i diversi regimi di rimborso degli Stati membri non devono rappresentare un ostacolo alla libera

---

[182] Art. 16, par. 4, TUE e dichiarazione relativa all'art. 16, par. 4, TUE e all'art. 238, par. 2, TFUE.

[183] Non si ignora, tuttavia, che tale scelta ha conseguenze sul diritto dell'Unione relativamente all'applicazione delle norme in materia di concorrenza e di aiuti di Stato. Cfr. sentenza della Corte del 24 aprile 2023, causa C-492/21 P, *Casa Regina Apostolorum*, ECLI:EU:C:2023:354. Per un commento alla sentenza della Corte, v. M. GUY, *Solidarity Rules? State Aid and Public Hospitals: Case C-492/21 P* Casa Apostolorum della Pia Società delle Figlie di San Paolo v. Commission, in *EU Law Live*, 2023.

[184] Tali modelli, infatti, riflettono l'assetto costituzionale e organizzativo dei singoli Stati. A questo proposito, vale la pena ricordare che nell'Unione è possibile distinguere tra il modello mutualistico (*Bismarck*), finanziato grazie ai contributi obbligatori dei lavoratori e dei datori di lavoro parametrati sullo stipendio, e il servizio sanitario nazionale (*Beveridge*), che si fonda sul sistema generale di tassazione: "[n]el primo le risorse sono gestite da imprese o fondi assicurativi indipendenti che si avvalgono di professionisti autonomi e offrono una serie limitata di servizi e trattamenti; nel secondo, invece, è lo Stato che amministra i fondi destinati alla sanità ed offre una copertura totale ai cittadini tramite strutture pubbliche" (G. DI FEDERICO, S. NEGRI, *op. cit.*, 2019, p. 65). Un'efficace descrizione dei modelli di organizzazione è fornita dall'Avvocato generale Geelhoed nelle conclusioni presentate il 15 dicembre 2005, in *Watts*, ECLI:EU:C:2005:784: "[all'interno della Comunità troviamo] sistemi a carattere interamente pubblico (come l'NHS del Regno Unito), sistemi ibridi (come il regime istituito dalla ZFW nei Paesi Bassi) e sistemi di assicurazione privati. Il finanziamento dei sistemi appartenenti alla prima categoria è interamente pubblico e le prestazioni sono erogate gratuitamente. I sistemi che rientrano nella seconda categoria possono essere finanziati da fonti pubbliche o private, ovvero da una combinazione di entrambe le fonti, mentre le prestazioni sono erogate in natura o in base ad un meccanismo di rimborso. Nel terzo modello, le prestazioni sono pagate direttamente dal paziente che viene successivamente rimborsato dalla propria assicurazione malattia. A seconda del tipo di organizzazione, tali sistemi avranno una gestione più rigida e saranno relativamente chiusi, ovvero avranno una gestione più flessibile e saranno relativamente aperti" (punto 21).

[185] Nella spiegazione alla proposta, la Commissione afferma chiaramente che questo strumento normativo non è pensato per "regolamentare le modalità con cui viene prestata l'assistenza sanitaria negli Stati membri" (COM(2022) 197 final, p. 9).

circolazione dei servizi di sanità digitale, come la telemedicina e i servizi farmaceutici online. Similmente, al fine di rafforzare l'interoperabilità e la sicurezza dei prodotti di sanità digitale, viene permesso agli Stati membri di mantenere e definire norme specifiche per l'appalto, il rimborso, il finanziamento o l'uso dei sistemi di cartelle cliniche elettroniche a livello nazionale nel contesto dell'organizzazione, erogazione e finanziamento dei servizi sanitari. Tuttavia, viene anche specificato che tali disposizioni nazionali non devono impedire la libera circolazione dei sistemi delle cartelle cliniche elettroniche all'interno dell'Unione [186].

La pressione sul livello nazionale aumenta ulteriormente se si considera l'uso da parte dell'Unione della leva finanziaria come strumento per indurre gli Stati membri a intraprendere con maggiore decisione la strada verso i cambiamenti strutturali, anche nelle politiche sanitarie [187]. Per beneficiare dei fondi del dispositivo per la ripresa e la resilienza [188], infatti, i piani nazionali dei singoli Stati membri (PNRR) devono già prevedere programmi di riforme

---

[186] Art. 29 e considerando 28 e 43 EHDS.

[187] Sull'uso della leva finanziaria per promuovere l'integrazione e influenzare le decisioni politiche nazionali, cfr. B. DE WITTE, *Integration through Funding – The Union's Finances as a Policy Instrument*, in R. WEBER (ed.), *The Financial Constitution of European Integration – Follow the Money?*, Hart Publishing, London, 2023, pp. 221-235; M. DAWSON, F. DE WITTE, *EU Law and Governance*, CUP, Cambridge, 2022, p. 89; P. DERMINE, *The Planning Method: An Inquiry into the Constitutional Ramifications of a New EU Governance Technique*, in *CMLRev*., 2024, vol. 61, p. 975. Con specifico riferimento all'ambito sanitario, cfr. Z. ZAPOTOCZNA, *The European Union's Influence on the Organisation of National Healthcare Systems. Navigating the Trends after the Covid-19 Pandemic*, in *EJHL*, 2025, vol. 32, pp. 1-25.

[188] Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza. Il crescente ruolo svolto dall'Unione in termini di politica di sanità pubblica può essere apprezzato anche guardando ai finanziamenti stanziati per la ricerca sanitaria. Nell'ambito del Quadro finanziario pluriennale, i fondi stanziati per la sanità comprendono strumenti quali il Fondo sociale europeo Plus (competenze del personale e migliore accesso all'assistenza sanitaria), il Fondo europeo di sviluppo regionale (infrastrutture, modernizzazione dei settori sanitari pubblico e privato e reti di cooperazione (inter)regionali, con investimenti in ricerca e innovazione, adozione di tecnologie avanzate e soluzioni innovative e nella digitalizzazione, anche in ambito sanitario), Orizzonte Europa (ricerca e innovazione in ambito sanitario), il programma Europa digitale (infrastrutture digitali a sostegno dell'uso delle tecnologie digitali in settori di interesse pubblico e infrastrutture di dati a sostegno di spazi di dati), il Meccanismo per collegare l'Europa 2.0 (reti gigabit altamente resilienti per collegare ospedali e centri medici, anche per la condivisione di dati medici) e il programma "UE per la salute" (EU4Health). Quest'ultimo programma, con un bilancio proposto di 5,1 miliardi di euro per il periodo 2021-2027, mira a "sostenere gli Stati membri nella transizione a una migliore preparazione e nel rafforzamento dei rispettivi sistemi sanitari e aiutarli a conseguire gli obiettivi di sviluppo sostenibile delle Nazioni Unite relativi alla salute" (COM(2020) 405 final, p. 1), nonché nell'attuazione dei principi del Pilastro europeo dei diritti sociali.

e investimenti in settori strategici [189], tra cui la transizione digitale e la salute [190]. Si aggiunga che i poteri di controllo sulla gestione dei fondi attribuiti all'Unione, formalmente conferiti per assicurare la corretta destinazione finalistica delle misure economiche, finiranno per incidere, *de facto*, su settori che rientrano nella sovranità degli Stati membri, tra cui l'organizzazione sanitaria (digitale) [191].

La spinta verso la digitalizzazione comporta l'introduzione a livello nazionale di strumenti digitali (ad es. FSE, infrastrutture ICT e stratificazione per la medicina di iniziativa) che consentano di rendere più sostenibile e di qualità il servizio sanitario, rafforzando la componente di sanità pubblica e delle cure primarie e intermedie (non ospedaliere). Simili cambi di rotta, seppur in parte frutto di operazioni di negoziazione, finiscono per toccare direttamente le prerogative nazionali di decidere in autonomia i modelli organizzativi e finanziari in ambito sanitario, enfatizzando le differenze nell'erogazione di prestazioni sanitarie non solo tra gli Stati membri, ma anche all'interno di uno stesso Stato, con evidenti ricadute in termini di disparità di trattamento offerto ai pazienti. Ad esempio, in sistemi come quello italiano, dove la sanità è regionalizzata, le proposte di riforma comportano novità significative per alcune regioni (ad es. Calabria e Campania), mentre si muovono su traiettorie di maggiore continuità per altre (ad es. l'Emilia-Romagna) [192].

---

[189] Cfr. L. CHIEFFI, *Equità nella salute e nei servizi sanitari tra politiche europee e interventi statali*, in *Corti Supreme*, 2022, vol. 1, p. 190. Vedi anche F. SALMONI, *Recovery fund, condizionalità e debito pubblico. La grande illusione*, Cedam, Padova, 2021, p. 27; L. CHIEFFI, *Una nuova stagione per i diritti sociali? La spinta offerta dal Recovery Fund per il rilancio dei welfare sanitari*, in *BioLaw Journal*, 2021, n. 4, p. 3 ss.; A. RIZZO, *La crisi pandemica e la nuova centralità delle politiche sanitarie europee alla luce della disciplina "EU4Health"*, in *SIE*, 2021, vol. 1, p. 107.

[190] R. MICCÙ, *op. cit*., 2021, p. 6 che sottolinea come "l'attesa riconfigurazione delle modalità di erogazione delle prestazioni sanitarie che deriva dagli atti europei di *hard* e di *soft law* è destinata a incidere tanto sul rapporto verticale tra gli iscritti al SSN e le reti territoriali di assistenza, quanto in quello orizzontale di attuazione della politica sanitaria interna, specie alla luce degli obiettivi che gli Stati membri dovranno diversamente raggiungere in attuazione dei *Recovery and Resilience National Plans*".

[191] *Ibid.* p. 11. L'A. evidenzia come gli Stati membri, in ragione del piano NGEU, siano beneficiari di "risorse *finalisticamente* condizionate, ossia funzionalizzate al raggiungimento degli obiettivi suggeriti dalla Commissione Ue nelle *country-specific recommendations* e indicati dallo Stato nel *National Recovery and Resilience Plan* 2021-23" (p. 11). Questa condizionalità di tipo teleologico, fondata sul raggiungimento di obiettivi fissati a livello nazionale, si distingue dal meccanismo di condizionalità economica del Semestre europeo. Sulla differenza tra il meccanismo della condizionalità e quello del Semestre europeo, si rinvia altresì a V. DELHOMME, T. HERVEY, *op. cit*., 2022, p. 72.

[192] Per un approfondimento sulle differenze nell'erogazione dei servizi sanitari tra regioni del Nord e del Sud Italia, si rinvia all'analisi di L. CHIEFFI, *op. cit*., 2022, p. 181 ss.

4.2. (*Segue*) Il sostegno degli *stakeholders* alle proposte della Commissione nel quadro delle consultazioni pubbliche

Le linee di intervento delineate dalla Commissione in vista dell'istituzione dello EHDS non hanno incontrato significative opposizioni nel corso della consultazione pubblica [193] avviata nel maggio 2021 e conclusasi nel luglio dello stesso anno [194]. Al contrario, come emerge dai risultati della consultazione, le proposte della Commissione hanno beneficiato di un sostegno ampio e trasversale da parte dei cittadini e dei portatori di interesse [195], i quali sono stati invitati a esprimere pareri sugli eventuali problemi da affrontare, sulle opzioni strategiche da scegliere e sul loro possibile impatto. Nello specifico, le consultazioni si sono concentrate su temi quali l'accesso ai dati sanitari e il loro uso per la fornitura di servizi di assistenza sanitaria, la ricerca e lo sviluppo, l'elaborazione delle politiche pubbliche e della regolamentazione, nonché la promozione di un mercato unico dei servizi e dei prodotti di sanità digitale (ad es. telemedicina e cartelle cliniche elettroniche).

---

[193] Art. 2 Protocollo n. 2 sull'applicazione dei principi di sussidiarietà e di proporzionalità. Quale espressione del principio di prossimità (art. 10, par. 3, TUE), questo strumento permette ai cittadini e ai portatori di interesse (ad es. autorità locali, regionali e nazionali, associazioni, società civile, imprese di diverse dimensioni e comunità scientifica) di contribuire al processo decisionale europeo al fine di migliorarne la qualità. Di recente, la Commissione si è impegnata a ridurre le fasi del processo di consultazione, con l'introduzione di un unico invito pubblicato sul portale web "Di' la tua", il miglioramento dei questionari e la consultazione del pubblico una sola volta nella fase di revisione di un atto legislativo, così da semplificare l'attuale sistema di consultazione e agevolare la presentazione di contributi da parte dei cittadini e dei portatori di interesse. Si è altresì insistito sull'importanza di fornire rapidamente ai partecipanti un feedback e aggiornamenti in merito agli sviluppi di ogni iniziativa (ad es. la pubblicazione della proposta della Commissione). Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Legiferare meglio: unire le forze per produrre leggi migliori, COM(2021) 219 final, del 29 aprile 2021, pp. 5-6.

[194] In questa occasione, Stella Kyriakides, commissaria per la Salute e la sicurezza alimentare, ha dichiarato che "[l]o spazio europeo dei dati sanitari sarà una componente fondamentale di un'Unione europea della salute forte e aprirà la strada a una collaborazione a livello di tutta l'UE per migliorare l'assistenza sanitaria, la ricerca e l'elaborazione delle politiche sanitarie". Oltre alle consultazioni avviate dalla Commissione, un ruolo centrale nella definizione di un quadro più chiaro della percezione dei cittadini e dei portatori di interesse rispetto alle questioni affrontate nella proposta è stato svolto nell'ambito del progetto "*Towards a European Health Data Space*", basato sul programma per la salute 2020 della Commissione.

[195] Anche nelle consultazioni pubbliche svoltesi in occasione delle iniziative legislative poste in essere nell'ambito della Strategia europea per i dati si registra una tendenza simile. Ad esempio, nella consultazione per il DGA, la Commissione ha ricevuto 806 contributi (COM(2020) 767 final, del 25 novembre 2020, p. 4), 449 per quella relativa al DA (COM(2022) 68 final, 23 febbraio 2022, p. 11) e 1215 per quella relativa all'AIA (COM(2021) 206 final, del 21 aprile 2021, p. 8).

Alla Commissione sono pervenute quasi quattrocento risposte valide provenienti in larga misura da cittadini europei, organizzazioni non governative e istituti universitari [196]. Pur con alcune differenze riconducibili alle diverse categorie di portatori di interesse [197], i risultati della consultazione mostrano un sostegno diffuso alle azioni dell'Unione "volte ad accelerare la ricerca in materia di salute (89 %), promuovere il controllo delle persone fisiche sui loro dati sanitari (88 %) e facilitare la prestazione di assistenza sanitaria transfrontaliera (83 %)" [198]. Più in generale il favore dei portatori di interesse riguarda tanto le misure relative all'accesso e allo scambio dei dati sanitari elettronici per finalità di uso primario e secondario, quanto quelle concernenti i servizi e i prodotti di sanità digitale [199].

La maggior parte degli intervistati ha individuato nella creazione di un'infrastruttura digitale a livello dell'Unione e nell'istituzione di un organismo europeo gli strumenti più idonei a facilitare l'accesso ai dati sanitari e la loro condivisione per finalità di uso secondario. Rispetto poi ai servizi e ai prodotti di sanità digitale, è emersa una marcata preferenza per l'introduzione di uno schema di certificazione a livello europeo volto a promuovere l'interoperabilità, nonché per la possibilità di integrare nei sistemi di cartelle cliniche elettroniche i dati raccolti da applicazioni di *mHealth* e da strumenti di telemedicina [200]. Particolarmente significativo è, inoltre, il consenso quasi unanime sull'opportunità di subordinare l'accesso ai fondi europei per la digitalizzazione dell'assistenza sanitaria al rispetto degli standard di interoperabilità fissati a livello europeo [201].

Il quadro che emerge dalle consultazioni pubbliche è dunque quello di un consenso ampio sulle finalità e sugli strumenti proposti dalla Commissione. Tale consenso, tuttavia, non si traduce necessariamente in una riflessione

---

[196] Gli Stati membri maggiormente attivi sono stati il Belgio, la Spagna, la Francia, la Germania e l'Italia.

[197] Queste risultano chiaramente dal report di sintesi della consultazione pubblica del 27 gennaio 2022, in cui vengono riportate, in particolare, quelle tra le società/organizzazioni aziendali e autorità pubbliche/istituti di ricerca (Ares(2022)636543, p. 3 ss.).

[198] COM(2022) 197 final, p. 11.

[199] Report di sintesi della consultazione pubblica del 27 gennaio 2022, Ares(2022)636543.

[200] COM(2022) 197 final, pp. 11-12. Tali dati sono confermati da una serie di altri studi condotti nei mesi precedenti la proposta della Commissione, nell'ambito dei quali sono state svolte ulteriori indagini tra i portatori di interesse: lo studio sulla valutazione delle norme nazionali sui dati sanitari alla luce del GDPR; l'analisi dei vuoti normativi relativi alla fornitura transfrontaliera di servizi e prodotti di sanità digitale, compresa l'intelligenza artificiale; uno studio sulle infrastrutture e l'ecosistema dei dati a sostegno della valutazione di impatto dello spazio europeo dei dati sanitari; e infine uno studio di valutazione d'impatto.

[201] Report di sintesi della consultazione pubblica del 27 gennaio 2022, Ares(2022)636543, p. 6.

critica sui limiti costituzionali dell'azione dell'Unione in ambito sanitario [202], ma sembra piuttosto accompagnare – e in parte legittimare – un'impostazione regolatoria fortemente orientata all'accentramento e all'armonizzazione, anche in settori tradizionalmente riservati agli Stati membri.

4.3. I limiti all'armonizzazione nel settore della sanità pubblica

Data l'assenza di un vincolo diretto sull'autonomia degli Stati membri – i quali, ad esempio, rimangono almeno formalmente liberi di non intraprendere un processo di digitalizzazione dei propri sistemi sanitari [203] –, difficilmente può sostenersi una violazione diretta dell'art. 168, par. 7, TFUE.

Tuttavia, permangono dubbi circa la piena compatibilità di alcune disposizioni dello EHDS con il quadro costituzionale europeo. Tali dubbi non discendono dall'esistenza di un divieto assoluto di armonizzazione nel settore della sanità pubblica, che non trova fondamento nel diritto primario. Come evidenziato in precedenza, infatti, l'art. 2, par. 5, TFUE non esclude che atti giuridicamente vincolanti adottati su basi giuridiche diverse possano incidere anche su settori nei quali l'Unione dispone di competenze di sostegno, coordinamento o completamento, purché tale incidenza resti funzionalmente subordinata agli obiettivi perseguiti da tali basi giuridiche e non si traduca in un intervento di armonizzazione settoriale in quanto tale.

Il nodo problematico posto dallo EHDS riguarda, piuttosto, l'intensità e l'estensione dell'armonizzazione realizzata, nonché il rapporto tra la base giuridica prescelta e il contenuto sostanziale dell'intervento. Sebbene formalmente

---

[202] Tra i molteplici contributi ricevuti, soltanto due hanno sollevato la questione delle limitate competenze di cui l'Unione dispone in questo settore. Tuttavia, in entrambi i casi, il quadro costituzionale delineato dai Trattati viene descritto come un ostacolo superabile alla luce delle potenzialità dello EHDS. Nella risposta dell'Organizzazione europea dei consumatori, ad esempio, si esorta la Commissione a individuare soluzioni idonee a promuovere l'armonizzazione degli approcci nazionali, nonché a stabilire un quadro giuridico comune per i servizi transfrontalieri di ricerca e assistenza sanitaria (*BEUC comments to Public consultation for legislative proposal on a European Health Data Space*, Ref. Ares(2021)4878924, del 26 luglio 2021). Analogamente, secondo il Consiglio europeo di optometria e ottica, dovrebbero essere individuati compromessi per fissare regole armonizzate in merito all'individuazione dei professionisti sanitari soggetti alle disposizioni dello EHDS (*Response by ECOO to the European Health Data Space Consultation*, Ref. Ares(2021)5516249, dell'8 settembre 2021).

[203] Si consideri, ad esempio, che l'obbligo imposto ai professionisti sanitari di registrare i dati *ex* art. 7 EHDS opera solo nel caso in cui i dati sanitari elettronici siano trattati per fornire assistenza sanitaria. Inoltre, pur se nei considerando, lo EHDS specifica che gli Stati mantengono la loro competenza "per quanto riguarda la registrazione iniziale dei dati sanitari elettronici personali, ad esempio subordinando la registrazione dei dati genetici al consenso della persona fisica o ad altre garanzie" (considerando 11 EHDS).

fondato sugli artt. 114 e 16, par. 2, TFUE, lo EHDS istituisce un *corpus* normativo dettagliato e direttamente applicabile che incide in modo strutturale sull'organizzazione, sul funzionamento e sulle priorità dei sistemi sanitari nazionali. In tale contesto, la tutela della salute non appare più come un obiettivo meramente accessorio rispetto al buon funzionamento del mercato interno o alla libera circolazione dei dati, bensì come una finalità autonoma e centrale dell'intervento normativo. È proprio questo scarto tra base giuridica formale e valenza materiale dell'armonizzazione a sollevare interrogativi circa la compatibilità dello EHDS con l'assetto delle competenze delineato dai Trattati.

Lo EHDS realizza infatti un livello di armonizzazione materiale particolarmente elevato, giustificato dalla Commissione alla luce dell'inadeguatezza delle misure di mero coordinamento della direttiva 2011/24/UE, caratterizzate da elementi di volontarietà e non vincolatività, nonché di alcune delle disposizioni del GDPR nel raggiungere obiettivi quali assicurare un maggiore controllo dei dati sanitari da parte delle persone fisiche e la libera circolazione dei dati sanitari nell'Unione. Di qui l'esigenza di adottare norme di armonizzazione per quanto riguarda l'uso primario e secondario dei dati sanitari elettronici, con implicazioni che si estendono ben oltre la dimensione transfrontaliera, incidendo anche su assetti normativi e organizzativi di rilievo puramente nazionale.

Per quanto riguarda l'uso primario dei dati sanitari, gli Stati membri sono obbligati a introdurre nuove disposizioni nazionali o a modificare quelle già vigenti, prevedendo, ad esempio, il passaggio da un sistema basato sul meccanismo di *opt-in* per la consultazione dei dati sanitari elettronici a uno fondato sull'*opt-out* [204]. Inoltre, al fine di garantire l'effettivo esercizio dei diritti delle persone fisiche in relazione a tale uso, è onere degli Stati membri predisporre servizi di accesso ai dati sia per i pazienti sia per i professionisti [205], nonché designare autorità di sanità digitale incaricate di monitorare il rispetto delle norme sull'uso primario dello EHDS [206], talvolta in collaborazione con le autorità di controllo per la protezione dei dati personali [207].

Ancora, con l'entrata in vigore dello EHDS, i dati sanitari elettronici, in particolare quelli elencati dall'art. 14 EHDS (ad es. i profili sanitari sintetici

---

[204] Art. 10 EHDS. Questo potrebbe essere il caso dell'ordinamento italiano, dove il consenso dell'interessato rappresenta il requisito necessario per la consultazione dei dati contenuti nel FSE (art. 8 decreto del Ministero della Salute del 7 settembre 2023, Fascicolo Sanitario Elettronico 2.0) e nell'EDS (art. 13 decreto recante Ecosistema Dati Sanitari, di cui all'articolo 12, comma 15-*quater* del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221 e successive modificazioni).

[205] Artt. 4 e 12 EHDS.

[206] Art. 19 EHDS.

[207] Art. 22 EHDS.

dei pazienti, le prescrizioni e le dispensazioni elettroniche, le immagini medicali e i risultati di laboratorio) [208], non potranno più essere scambiati secondo specifiche tecniche nazionali, ma dovranno conformarsi al formato di scambio europeo delle cartelle cliniche elettroniche [209]. Questo obbligo mira, tra le altre cose, a garantire ai cittadini il diritto di ottenere una copia dei loro dati sanitari elettronici [210] e di richiedere al titolare la trasmissione degli stessi a un destinatario situato in un altro Stato membro, qualora i dati sanitari in questione rientrino tra le categorie prioritarie di cui all'art. 14 EHDS [211].

Grazie alle novità introdotte dallo EHDS dovrebbe quindi essere possibile superare gli ostacoli che finora hanno limitato l'effettivo esercizio, da parte delle persone fisiche, dei diritti relativi all'accesso e alla trasmissione dei propri dati. Tali ostacoli derivano dalle differenze tra gli ordinamenti nazionali nell'attuazione dei diritti riconosciuti dal GDPR – in particolare, il diritto di accesso e il diritto alla portabilità –, nonché dai ritardi nell'attuazione della piattaforma MyHealth@EU a livello nazionale e dal limitato ricorso, da parte degli Stati membri, alle norme e alle specifiche del formato europeo di scambio delle cartelle cliniche elettroniche.

Da un lato, infatti, il GDPR, pur essendo un regolamento e quindi direttamente applicabile, concede agli Stati membri un significativo margine di discrezionalità nell'attuazione concreta di alcuni diritti delle persone fisiche rispetto al trattamento dei loro dati [212]. Dall'altro, la direttiva 2011/24/UE si limita a raccomandare la cooperazione tra la Commissione e gli Stati membri per promuovere una maggiore interoperabilità tra i formati e gli standard utilizzati per la prestazione di cure sanitarie che si avvalgono delle Tecnologie dell'Informazione e della Comunicazione (TIC), e per agevolare l'accesso dei

---

[208] Tali categorie di dati sanitari elettronici corrispondono ai domini delle informazioni sanitarie per lo scambio transfrontaliero, indicati nella raccomandazione 2019/243, punto 2.1 e qualificati come prioritari dalla rete di assistenza sanitaria online, sulla base delle attuali attività nell'ambito dell'infrastruttura di servizi digitali per l'*eHealth* e della pertinenza clinica per l'assistenza sanitaria transfrontaliera. La formulazione dell'art. 14 EHDS rende evidente come l'elenco ivi previsto sia tutt'altro che tassativo. Difatti, è ammesso che gli Stati lo integrino aggiungendo altre categorie di dati sanitari elettronici (art. 14, par. 1, EHDS).

[209] Ai sensi dell'art. 15 EHDS, il formato di scambio delle cartelle cliniche elettroniche consiste in un formato strutturato, di uso comune e leggibile da un dispositivo automatico che consente la trasmissione di dati sanitari elettronici personali tra applicazioni software, dispositivi e prestatori di assistenza sanitaria diversi. La fissazione delle specifiche tecniche sul formato europeo di scambio spetta alla Commissione tramite atti di esecuzione che permettono, in questo caso, previa consultazione dei rappresentanti degli Stati membri, di fissare condizioni uniformi per l'applicazione dell'atto in tutta l'Unione.

[210] Art. 3 EHDS.

[211] Art. 7 EHDS.

[212] Art. 23 GDPR. Sul punto, si rimanda all'analisi svolta nella sezione 3.2.1 del capitolo 4.

pazienti ad applicazioni di assistenza sanitaria online, qualora adottati a livello nazionale [213]. Tra gli strumenti giuridici non vincolanti adottati in attuazione della direttiva 2011/24/UE si annoverano la raccomandazione sull'interoperabilità dei sistemi di cartelle cliniche elettroniche e, più di recente, la raccomandazione 2019/243 sul formato europeo di scambio delle cartelle cliniche elettroniche. Quest'ultima, tra le altre cose, consente agli Stati membri di continuare ad applicare le specifiche nazionali esistenti per i sistemi di cartelle cliniche elettroniche in parallelo al formato europeo di scambio.

Passando poi all'uso secondario dei dati sanitari elettronici, lo EHDS impone un obbligo per i titolari dei dati (ad es. gli ospedali e i professionisti sanitari) [214] di mettere a disposizione alcune categorie di dati sanitari elettronici (ad es. i dati derivanti da cartelle cliniche elettroniche e i dati sanitari generati dalla persona tramite dispositivi medici e applicazioni di sanità digitale) [215], per specifiche finalità [216]. La previsione di tale obbligo implica per gli Stati membri la necessità di designare organismi responsabili per l'accesso ai dati, incaricati, tra le altre cose, di decidere sulle domande di accesso ai dati e sulle richieste di dati [217]. Di conseguenza, per poter accedere ai dati sanitari in formato elettronico, sarà necessario seguire procedure armonizzate a livello europeo [218].

Attraverso l'istituzione di un quadro normativo armonizzato per la condivisione dei dati sanitari elettronici, il legislatore europeo ha riempito di contenuto le eccezioni di cui all'art. 9, par. 2, lett. g)-j), GDPR, obbligando gli Stati membri a rivedere i loro approcci all'uso dei dati per finalità di programmazione sanitaria, ricerca e valorizzazione economica. L'eccessivo ricorso, a livello nazionale, alle disposizioni di specificazione facoltative del GDPR ha infatti provocato una situazione di frammentazione che ha reso difficile, se non impossibile, l'accesso ai dati sanitari, limitando l'opportunità "per ricercatori, innovatori, responsabili delle politiche e regolatori di eseguire i loro compiti o di svolgere attività di ricerca o di innovazione" [219].

---

[213] Raccomandazione (UE) 2019/243 della Commissione relativa a un formato europeo di scambio delle cartelle cliniche elettroniche, del 6 febbraio 2019.

[214] Sono esentati da tale obbligo solo i singoli ricercatori, le persone fisiche, nonché le persone giuridiche che rientrano nella nozione di micro-imprese *ex* art. 2, all. alla raccomandazione della Commissione 2003/361/CE, salvo che il diritto nazionale non disponga diversamente (art. 50 EHDS).

[215] Art. 51 EHDS.

[216] Artt. 53-54 EHDS.

[217] Artt. 55 e 57, par. 1, lett. a), EHDS.

[218] Artt. 68-69 e 72 EHDS. Per una descrizione dettagliata di tali procedure, si rinvia alla sezione 3.1.2 del capitolo 3.

[219] COM(2022) 197 final, p. 8

Oltre alle norme dello EHDS menzionate sino ad ora, l'incisività dell'intervento dell'Unione a livello nazionale emerge anche dalle disposizioni relative alla partecipazione obbligatoria alle infrastrutture MyHealth@EU e HealthData@EU. Entrambe sono concepite per collegare i punti di contatto nazionali con le piattaforme centrali, rispettivamente, per la sanità digitale e per l'uso secondario dei dati sanitari elettronici.

Tramite MyHealth@EU, la Commissione fornisce servizi di scambio di dati sanitari di cui all'art. 14 EHDS sulla base del formato europeo di scambio delle cartelle cliniche elettroniche [220]. Rispetto alla direttiva 2011/24/UE, la partecipazione degli Stati a tale infrastruttura non è più volontaria, bensì obbligatoria. Di conseguenza, tutti gli Stati membri devono aderirvi, assicurandosi che i prestatori di assistenza sanitaria siano collegati ai rispettivi punti di contatto e siano in grado di effettuare uno scambio bidirezionale di dati sanitari elettronici, e che le farmacie riescano a dispensare le prescrizioni elettroniche rilasciate da altri Stati membri [221].

Con l'infrastruttura HealthData@EU, oltre ai servizi di scambio di informazioni tra gli organismi responsabili dell'accesso ai dati e i partecipanti autorizzati per le richieste di accesso transfrontaliero, la Commissione può offrire servizi ulteriori, come il mantenimento di cataloghi di dati accessibili, l'istituzione di un ambiente sicuro per la trasmissione e l'analisi dei dati provenienti da infrastrutture nazionali differenti e il collegamento tra lo EHDS e gli altri spazi comuni europei di dati (ad es. ambientale, sociale e agricolo) [222].

Dall'analisi appena compiuta appare dunque evidente un'inversione di tendenza netta nell'approccio regolatorio adottato dal legislatore in materia di sanità digitale. Con la direttiva 2011/24/UE e il GDPR, si è evitato di procedere a un'armonizzazione completa in un ambito caratterizzato da forti interessi nazionali. In particolare, la direttiva 2011/24/UE si limita a rafforzare la cooperazione tra i prestatori di assistenza sanitaria, i fruitori e le autorità di regolamentazione dei vari Stati membri, non tramite misure di armonizzazione, bensì tramite l'adozione di atti giuridici non vincolanti (ad es. orientamenti e raccomandazioni) relativi a: i) il riconoscimento delle prescrizioni rilasciate in altri Stati membri [223], ii) lo sviluppo di reti di riferimento europee

[220] Art. 23 EHDS.

[221] Art. 23, parr. 5-6, EHDS. Sempre nell'ambito dell'uso primario dei dati sanitari elettronici, ma senza fissare un obbligo specifico, gli Stati membri possono erogare servizi supplementari (ad es. servizi di telemedicina e sanità mobile). In più, insieme alla Commissione, possono agevolare lo scambio di dati sanitari elettronici con altre infrastrutture (ad es. il sistema di gestione dei dati clinici dei pazienti) (art. 24, parr. 1-2, EHDS).

[222] Artt. 75, parr. 8, 9 e 11, e 79 EHDS.

[223] Art. 11, par. 2, lett. b), direttiva 2011/24/UE.

tra prestatori di assistenza sanitaria e centri di eccellenza [224], iii) lo scambio di informazioni tramite la rete di assistenza sanitaria online [225], e iv) la valutazione delle tecnologie sanitarie [226]. Similmente, il GDPR lascia un certo margine di apprezzamento agli Stati membri per quanto riguarda sia i diritti delle persone fisiche sia il trattamento dei loro dati, specialmente per finalità di ricerca scientifica [227].

Al contrario, con lo EHDS, il legislatore europeo non sembra porsi eccessivi scrupoli nell'armonizzare questo settore, predisponendo un intervento di intensità medio-alta, sulla base della necessità di dare finalmente realizzazione a obiettivi che il quadro giuridico esistente non aveva consentito di raggiungere. Tra le opzioni strategiche elaborate dalla Commissione nel corso della valutazione d'impatto [228], la scelta è ricaduta su un modello regolatorio che non si fonda più su strumenti volontari o meccanismi di cooperazione rafforzata, ma che stabilisce norme armonizzate per l'accesso ai dati sanitari elettronici e per il loro uso (primario e secondario) non solo a livello europeo, ma anche a livello nazionale. In questa prospettiva, può essere letta anche la scelta di superare i limiti delle discipline precedenti, abbandonando lo strumento della direttiva – vera e propria o, nel caso del GDPR, "mascherata" [229] – a favore del regolamento, pensato per rafforzare "l'economia dei dati sanitari dell'UE aumentando la certezza del diritto e garantendo un quadro giuridico settoriale completamente uniforme e coerente" [230].

---

[224] Art. 12, par. 6, direttiva 2011/24/UE.

[225] Art. 14, direttiva 2011/24/UE.

[226] Art. 15 direttiva 2011/24/UE.

[227] Tali aspetti verranno affrontati più diffusamente nel capitolo 4.

[228] Secondo l'accordo interistituzionale Legiferare meglio del 2016, durante la valutazione d'impatto, le istituzioni possono verificare la conformità dei principi di sussidiarietà, proporzionalità e il rispetto dei diritti fondamentali. Sull'accordo interistituzionale e sulla valutazione d'impatto, cfr. M. DAWSON, *Better Regulation and the Future of EU Regulatory Law and Politics*, in *CMLRev*., 2016, vol. 53, n. 5, pp. 1209-1236; C. TOVO, *I nuovi equilibri tra potere esecutivo e legislativo nell'Unione europea: l'accordo interistituzionale "Legiferare meglio"*, in *Eurojus*, 2016, pp. 1-9.

[229] Così come approfondiremo nel capitolo 4 (v. in particolare, nota 35), il termine di direttiva "mascherata" associato al GDPR viene utilizzato con riferimento a quelle disposizioni che, lasciando ampio margine di manovra agli Stati membri, hanno contribuito alla creazione di un quadro normativo estremamente frammentato in materia.

[230] COM(2022) 197 final, p. 9.

4.4. (*Segue*) La voce flebile dei Parlamenti nazionali nell'ambito dei pareri del Protocollo n. 2 e del dialogo politico

Come già evidenziato con riferimento all'autonomia nazionale in ambito sanitario [231], anche rispetto all'intervento di armonizzazione operato dal legislatore europeo attraverso lo EHDS, gli Stati membri non hanno avanzato osservazioni. In particolare, i Parlamenti nazionali non si sono avvalsi dello strumento che consente loro di presentare pareri e osservazioni nel corso del processo di adozione degli atti dell'Unione [232]. Com'è noto, infatti, una volta che sono stati ricevuti i progetti legislativi delle istituzioni [233], i documenti di consultazione della Commissione [234] e i calendari di lavoro di quest'ultima e del Consiglio [235], i Parlamenti nazionali possono inviare ai presidenti del Parlamento europeo, del Consiglio e della Commissione un parere motivato contenente le ragioni per cui si ritiene che il progetto in questione violi il principio di sussidiarietà (c.d. sistema dell'allarme preventivo) [236]. Oltre a questa tipologia

---

[231] Cfr. sezione 4.2.

[232] Sulla partecipazione dei Parlamenti nazionali in ambito sanitario, cfr. F. COSTAMAGNA, *op. cit*., 2011, p. 188. Più in generale, invece, si rinvia a C. CECCHETTI, *Il controllo dei parlamenti nazionali sul rispetto del principio di sussidiarietà*, in G. DI FEDERICO (a cura di), *Alla (ri)scoperta del Parlamento europeo: 1979-2019*, Giappichelli, Torino, 2021, pp. 181-203; O. PORCHIA, *La sussidiarietà attraverso il riordino delle competenze? Il Trattato di riforma e la ripartizione delle competenze*, in *SIE*, 2010, vol. 3, pp. 642-646; S. DE BELLIS, *L'interazione fra parlamenti nazionali e le istituzioni comunitarie dopo Lisbona*, in *SIE*, 2010, vol. 3, pp. 621-623; L. GIANNITI, R. MATROIANNI, *Il ruolo dei parlamenti nazionali*, in F. BASSANINI, G. TIBERI (a cura di), *Le nuove istituzioni europee. Commento al Trattato di Lisbona*, Il Mulino, Bologna, 2008, pp. 161-183; J-V. LOUIS, *National Parliaments and the Principle of Subsidiarity: Legal Options and Practical Limits*, in *Eur. Const. Law Rev.*, 2008, vol. 15, pp. 429-458; W. SLEATH, *The Role of National Parliaments in European Affairs*, in G. AMATO, H. BRIBOSIA, B. DE WITTE (eds.), *Genèse et destinée de la Constitution européenne: commentaire du traité établissons une Constitution pour l'Europe à la lumière des travaux préparatoires et perspectives d'avenir*, Bruylant, Brussels, 2007, pp. 545-564; R. MASTROIANNI, *Le competenze dell'Unione*, in G. MORBIDELLI, F. DONATI (a cura di), *Una Costituzione per l'Unione europea*, Giappichelli, Torino, 2006, pp. 148-154; R. CAFARI PANICO, *Principio di sussidiarietà e clausola di flessibilità*, in G. ADINOLFI, A. LANG (a cura di), *Il Trattato che adotta una Costituzione per l'Europa: quali limitazioni all'esercizio dei poteri sovrani degli Stati?*, Giuffrè, Milano, 2006, pp. 102-109.

[233] Art. 12, lett. a), TUE. Ai sensi dell'art. 2.2 Protocollo n. 1 e art. 4 Protocollo n. 2, con "progetto di atto legislativo" si intende "la proposta della Commissione, l'iniziativa di un gruppo di Stati membri, l'iniziativa del Parlamento europeo, la richiesta della Corte di giustizia, la raccomandazione della Banca centrale europea e la richiesta della Banca europea per gli investimenti, intese all'adozione di un atto legislativo".

[234] Art. 1 Protocollo n. 1.

[235] Art. 5 Protocollo n. 1.

[236] Art. 3 Protocollo n. 1 e art. 6 Protocollo n. 2. Merita ricordare che, oltre al controllo politico dei Parlamenti nazionali sul rispetto del principio di sussidiarietà secondo le procedure

di pareri motivati prevista dal Protocollo n. 2, i Parlamenti nazionali hanno la possibilità, sin da prima del Trattato di Lisbona, di presentare osservazioni nel contesto del c.d. "dialogo politico" [237], anche detto "*Barroso Initiative*" [238].

Le due tipologie di pareri si distinguono quanto al termine entro cui devono essere presentati, agli effetti giuridici che producono e al loro contenuto. Solo i pareri ex Protocollo n. 2 devono essere inviati alle istituzioni entro otto settimane dalla data di trasmissione formale del progetto di atto legislativo (con alcune eccezioni per quanto riguarda il periodo estivo e quello invernale) e impongono alle istituzioni di "tenere conto" dei pareri o, qualora siano raggiunte soglie specifiche, calcolate sulla base dei voti attribuiti ai Parlamenti nazionali, di riesaminare tali progetti [239]. Con riferimento al contenuto, in linea teorica, i pareri presentati nell'ambito del dialogo politico possono riguardare aspetti ulteriori rispetto al controllo di sussidiarietà, mentre quelli ex

---

stabilite dal Protocollo n. 2, l'ordinamento europeo prevede un controllo giurisdizionale da parte dei giudici della Corte. Questi ultimi devono verificare tanto il rispetto delle garanzie procedurali di cui al Protocollo n. 2, quanto le condizioni sostanziali fissate dall'art. 5, par. 3, TUE. Cfr. E. CANNIZZARO, *op. cit.*, 2022, pp. 289-293.

[237] Comunicazione della Commissione al Consiglio europeo, Un'agenda dei cittadini. Per un'Europa dei risultati, COM(2006) 211 final, del 10 maggio 2006, p. 9 ss.

[238] D. JANCIC, *The Barroso Initiative: Window Dressing or Democracy Boost?*, in *Utrecht L. Rev*., 2012, vol. 8, p. 78.

[239] Nei sistemi bicamerali, ciascuna camera dispone di un voto (art. 7, par. 1, Protocollo n. 2). L'art. 7 Protocollo n. 2 descrive le procedure di "cartellino giallo" e "cartellino arancione". Secondo la prima, la Commissione è tenuta a riesaminare la sua proposta nel caso in cui i pareri motivati rappresentino almeno un terzo dell'insieme dei voti attribuiti ai Parlamenti nazionali (pari a 18 voti a seguito dell'uscita del Regno Unito dall'Unione europea). Tale soglia è abbassata a un quarto dei voti quando il progetto di atto legislativo si fonda sull'art. 76 TFUE relativo allo spazio di libertà, sicurezza e giustizia (art. 7, par. 2, Protocollo n. 2). Sulla base della seconda procedura, invece, la Commissione è soggetta a un obbligo di riesame più approfondito rispetto a quello previsto per la procedura di "cartellino giallo" quando i pareri motivati rappresentano la maggioranza semplice dei voti (oggi pari a 28) e il progetto deve essere adottato secondo la procedura legislativa ordinaria (art. 7, par. 3, comma 1, Protocollo n. 2). Anche in questa ipotesi, l'istituzione proponente può decidere di mantenere, modificare o ritirare la proposta ma, qualora decidesse di mantenerla, diversamente dalla procedura di "cartellino giallo", è obbligata a indicare le ragioni di tale scelta in un parere motivato che viene sottoposto, insieme ai pareri motivati dei Parlamenti nazionali, al Parlamento europeo e al Consiglio (art. 7, par. 3, comma 2, Protocollo n. 2). Si noti come, di recente, il Parlamento europeo abbia proposto di "rafforzare il controllo della sussidiarietà da parte della Corte di giustizia dell'Unione europea", chiedendo di tenere conto "del parere dei parlamenti regionali con poteri legislativi nei pareri motivati dei Parlamenti nazionali riguardanti i progetti legislativi; […] di estendere a 12 settimane il termine per la procedura del cartellino giallo", nonché di "introdurre un meccanismo del cartellino verde per le proposte legislative dei Parlamenti nazionali o regionali con poteri legislativi, al fine di adeguare meglio il diritto dell'Unione alle esigenze locali". Cfr. Risoluzione del Parlamento europeo sui progetti del Parlamento europeo intesi a modificare i Trattati (2022/2051(INL)), del 22 novembre 2023, p. 5.

Protocollo n. 2 dovrebbero riguardare la sola verifica del principio di sussidiarietà e quindi limitarsi a valutare l'insufficienza dell'azione degli Stati membri (*negative test*) e il valore aggiunto di quella dell'Unione (*positive test*) [240]. Tuttavia, tale controllo spesso sconfina nella verifica del rispetto del principio di proporzionalità [241] o in un più generale esame sulla presa in considerazione da parte dell'Unione delle specificità nazionali [242].

Le relazioni annuali della Commissione sull'applicazione dei principi di sussidiarietà e proporzionalità degli ultimi anni mostrano una generale tendenza da parte dei Parlamenti nazionali a privilegiare il canale del dialogo politico, piuttosto che del controllo di sussidiarietà ex Protocollo n. 2 [243]. Così è accaduto anche per la proposta dello EHDS, rispetto alla quale si sono espressi unicamente [244] il Parlamento portoghese e la Camera dei deputati e il Senato della Repubblica ceca [245]. Il Parlamento portoghese ha presentato un parere in cui rileva la piena conformità della proposta ai principi di sussidiarietà e proporzionalità [246]. Alla stessa conclusione giungono anche la Camera

---

[240] Recentemente, il Tribunale dell'Unione ha ribadito che la verifica del rispetto del principio di sussidiarietà si compone di un "*negative test*" per valutare che gli obiettivi perseguiti non possono essere adeguatamente realizzati dai soli Stati membri, e di un "*positive test*" per controllare che tali obiettivi, per portata ed effetti, possono essere realizzati meglio a livello dell'Unione. Cfr. sentenza del Tribunale del 13 luglio 2022, causa T-227/21, *Illumina c. Commissione*, ECLI:EU:T:2022:447, punto 158, poi appellate davanti alla Corte di giustizia nella causa C-611/22 P, ECLI:EU:C:2023:205. Per una differente qualificazione dei due test, si veda R. SCHÜTZE, *op. cit.*, 2009, p. 250 che parla di "*national insufficiency test*", secondo cui l'Unione può intervenire solo quando gli obiettivi da perseguire non possono essere adeguatamente raggiunti dai singoli Stati membri, e "*comparative efficiency test*", che esclude l'azione dell'Unione a meno che essa non si trovi nella posizione migliore per conseguire gli scopi prefissati.

[241] La Corte ha riconosciuto tale difficoltà nella sentenza *British American Tobacco*, punto 184. Per un approfondimento v., in dottrina, S. WEATHERILL, *op. cit.*, 2011, pp. 857-858, T. TRIDIMAS, *General Principles of EU Law*, OUP, Oxford, 2006, p. 176, e P. DE PASQUALE, *Commento all'articolo 5 TUE*, in A. TIZZANO (a cura di), *op. cit.*, 2014, p. 50.

[242] Cfr. relazione annuale 2022 della Commissione sull'applicazione dei principi di sussidiarietà e proporzionalità e sulle relazioni con i parlamenti nazionali, COM(2023) 640 final, del 12 ottobre 2023, p. 9.

[243] Le concause di tale tendenza sono state efficacemente illustrate da L. CECCHETTI, *op. cit*., 2021, p. 204 ss.

[244] Per completezza, secondo quanto riportato nel documento del servizio di ricerca del Parlamento europeo, sembra che anche la Francia abbia presentato un parere sulla proposta di regolamento sullo EHDS (*Legislative Brief European Health Data Space*, 2024, p. 9). Tuttavia, al momento, tale parere non risulta essere disponibile nella sezione dedicata del sito EUR-Lex: https://eur-lex.europa.eu/legal-content/IT/HIS/?uri=celex%3A52022PC0197.

[245] Questo dato è parzialmente in linea con quanto è avvenuto per gli atti proposti nell'ambito della Strategia europea per i dati, rispetto alle cui proposte sono stati presentati tra i tre (DA) e quattro pareri da parte dei Parlamenti nazionali (AIA e DGA).

[246] Parere del 21 luglio 2022 sull'applicazione dei principi di sussidiarietà e proporzionalità,

dei deputati e il Senato cechi che, tuttavia, nelle due risoluzioni presentate, sollevano una serie puntuale di questioni di carattere sostanziale [247].

Nelle risoluzioni del Parlamento ceco vengono messi fortemente in discussione i vantaggi che, secondo la Commissione, dovrebbero derivare dall'adozione del regolamento sullo EHDS (ad es. qualità dell'assistenza e vantaggi finanziari per le strutture sanitarie), evidenziandone i rischi, tra cui la deumanizzazione del rapporto medico-paziente e l'uso improprio dei dati sanitari. Il Parlamento della Repubblica Ceca esprime altresì preoccupazioni in merito all'impatto che il passaggio a sistemi di cartelle cliniche elettroniche avrà sulle strutture sanitarie sia dal punto di vista finanziario, sia da quello organizzativo ed educativo. In più, vengono espresse perplessità sul modo in cui evitare l'esclusione dal sistema sanitario nazionale di coloro che hanno deciso di non condividere i propri dati con altre strutture sanitarie o di metterli a disposizione dello EHDS. La proposta, infatti, non sembra ammettere la possibilità di utilizzare un metodo per scambiarsi i dati sanitari diverso da quello individuato nello EHDS.

Nessuna critica, invece, viene mossa alla motivazione fornita dalla proposta quanto al rispetto del principio di sussidiarietà [248]. Sebbene le istituzioni dell'Unione godano di un certo margine di apprezzamento nello svolgere il test di sussidiarietà [249], il contenuto della proposta è piuttosto scarno nel dimostrare in che modo l'azione a livello dell'Unione possa conseguire risultati migliori [250].

---

p. 7: secondo il Parlamento portoghese la proposta è conforme al principio di sussidiarietà in quanto gli obiettivi che persegue non possono essere raggiunti unilateralmente da nessuno Stato membro o bilateralmente tra Stati membri, ma solo a livello di Unione europea.

[247] Le questioni sollevate dal Parlamento della Repubblica Ceca riguardano sia l'uso primario sia quello secondario dei dati sanitari elettronici. Ad esempio, viene contestata l'assenza di un diritto della persona fisica a non condividere i propri dati sanitari elettronici e viene rilevata la difficoltà nel distinguere tra "*research for social well-being*" e "*research for the potentially or deliberately dangerous*", con particolare riguardo agli ambiti della genetica e dell'IA.

[248] Questo dato non sorprende se si considera la scelta della base giuridica dello EHDS. A questo proposito, la dottrina ha da tempo sottolineato la sostanziale inefficacia del controllo sulla sussidiarietà di una misura adottata per motivi legati al mercato interno, che richiede un livello di armonizzazione raggiungibile solo dall'Unione. Di conseguenza, anche se gli Stati membri potrebbero assicurare meglio gli obiettivi di salute, l'Unione sarà comunque in una posizione migliore per realizzare entrambi gli obiettivi. Cfr. E. CANNIZZARO, *op. cit.*, 2022, p. 291; V. DELHOMME, *Emancipating Health from Internal Market: For a Stronger EU (Legislative) Competence in Public Health*, in *Eur. J. Risk Regul.*, 2020, vol. 11, fasc. 4, p. 753; G. DAVIES, *op. cit.*, 2006, pp. 63-84.

[249] Cfr., ad esempio, la sentenza della Corte *Philip Morris*, punto 218 e le sentenze dell'8 giugno 2010, causa C-58/08, *Vodafone*, ECLI: ECLI:EU:C:2010:321, punto 72; del 9 ottobre 2001, causa C-377/98, *Paesi Bassi/Parlamento e Consiglio*, ECLI:EU:C:2001:523, punto 32.

[250] Una descrizione più particolareggiata quanto alla conformità ai principi di sussidiarietà e di proporzionalità si trova nella griglia sul rispetto del principio di sussidiarietà e nella

Questo elemento risulta problematico perché l'obbligo di motivazione degli atti giuridici di cui all'art. 296 TFUE è funzionale non solo a fare in modo che la Corte possa esercitare il proprio controllo sull'attività legislativa delle istituzioni, ma anche affinché gli Stati membri e i cittadini interessati siano informati sulle condizioni alle quali le istituzioni dell'Unione hanno fatto applicazione del Trattato [251].

In aggiunta, nessun dubbio viene mosso in riferimento all'adeguatezza della base giuridica o del tipo di atto legislativo scelto. Non vi sono osservazioni nemmeno sul livello di armonizzazione introdotto e sull'eventualità che questo possa pregiudicare l'autonomia riconosciuta agli Stati membri nel settore della sanità pubblica e nell'applicazione del diritto dell'Unione. Similmente, non vengono sollevate perplessità sul rispetto delle specificità nazionali relativamente alla regolamentazione di profili etici legati all'uso dei dati sanitari elettronici e alla digitalizzazione dell'assistenza sanitaria e, più in generale, di aspetti che rientrano nella c.d. clausola identitaria di cui all'art. 4, par. 2, TUE (ad es. le differenti concezioni del diritto alla salute e della dignità umana).

Rilievi di questo tipo da parte dei Parlamenti nazionali avrebbero contribuito ad arricchire e orientare le successive fasi di negoziazione dell'atto tra le istituzioni dell'Unione. Queste ultime, assistite da organi consultivi come il Comitato economico e sociale europeo (CESE) e il Comitato delle regioni (CdR), si fanno portatrici di istanze specifiche che, nel corso del dialogo interistituzionale, trovano una sintesi nel testo finale dell'atto [252].

---

valutazione d'impatto, la quale, secondo la giurisprudenza della Corte, è pertinente ai fini del controllo della compatibilità dell'atto con il principio di proporzionalità (sentenza *Vodafone*, punto 55) e di sussidiarietà (sentenza *Philip Morris*, punto 226). Vale la pena anche notare che, in seguito al primo parere negativo del Comitato di controllo normativo (SEC(2022)196, del 26 gennaio 2022, pp. 7-8), la Commissione ha ampliato la spiegazione relativa alla base giuridica e al rispetto dei principi di sussidiarietà e proporzionalità. Per ulteriori approfondimenti in merito, si rinvia anche a DG Sante, *Study Supporting the Impact Assessment of Policy Options for an EU Initiative on a European Health Data Space*, 2022 e F. LUPIÁÑEZ-VILLANUEVA et al., *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, 2021.

[251] Sentenza della Corte del 13 maggio 1997, causa C-233/94, *Germania/Parlamento e Consiglio*, ECLI:EU:C:1997:231, punto 25. Tuttavia, non si ignora che, nella stessa sentenza, viene riconosciuta la possibilità che anche una motivazione implicita costituisca una giustificazione sufficiente del rispetto del principio di sussidiarietà (punto 28). Più di recente, la Corte ha altresì sottolineato che l'adempimento dell'obbligo di motivazione può essere valutato alla luce del contesto e delle circostanze del caso di specie, oltre che del tenore dell'atto contestato. Cfr. sentenza *Philip Morris*, punto 225.

[252] Se da un lato il Parlamento e il Consiglio sono sensibili alle rivendicazioni nazionali avanzate, rispettivamente, dai cittadini e dai loro governi (art. 10, par. 2, TUE), dall'altro la Commissione è tendenzialmente favorevole a una maggiore integrazione europea. Inoltre, il CESE e il CdR, nello svolgere la loro attività consultiva, fungono da ponte tra le istituzioni e

Se si guarda alle posizioni del Consiglio e del Parlamento europeo nel corso dell'iter legislativo [253] e le si confronta con il testo iniziale della proposta dello EHDS, sono diverse le disposizioni su cui i co-legislatori sono intervenuti, anche su impulso del CESE e CdR. Questi ultimi, pur riconoscendo l'insufficienza dell'azione degli Stati membri e il valore aggiunto di quella dell'Unione [254], invitano i legislatori a procedere con prudenza, tenendo in considerazione che vi sono "*too many challenges ahead when we talk about the Member States' health systems. There are different paces, different views about public and private health systems and citizens must realise that this proposal means investment and public policy choices*" [255]. Di conseguenza, essi ritengono che lo EHDS non dovrebbe consentire all'Unione di eccedere rispetto alle competenze che le sono state attribuite, rispettando "*the rights of Member States and/or regional or local authorities with regard to the organisation of healthcare, given that a number of countries have chosen to devolve various responsibilities for healthcare to regional or local authorities, allowing decisions to be taken as closely as possible to citizens*" [256].

In questa direzione vanno molte delle modifiche proposte al testo dello EHDS da parte del CdR, parzialmente fatte proprie dal Consiglio e non, invece, dal Parlamento europeo [257]. Quanto all'uso primario dei dati sanitari

---

i cittadini dell'Unione. Indicati dai governi nazionali e nominati dal Consiglio dell'Unione, i componenti del CESE e del CdR contribuiscono affinché le istanze, rispettivamente, delle organizzazioni dei lavoratori, dei datori di lavoro e di altri gruppi di interesse (ad es. gli agricoltori e i consumatori) e degli enti regionali e locali possano trovare espressione nel corso del dialogo politico.

[253] In particolare, il 6 dicembre 2023 il Consiglio ha adottato il suo *general approach* (di seguito, *general approach* del Consiglio), mentre il 13 dicembre 2023 il Parlamento europeo ha approvato il report adottato congiuntamente dalle commissioni LIBE ed ENVI a fine novembre 2023 (di seguito, report del Parlamento).

[254] Si veda, ad esempio, il parere del CdR dell'8 febbraio 2023 in cui la proposta viene ritenuta conforme al principio di sussidiarietà dal momento che obiettivi relativi alla portabilità e all'interoperabilità dei dati "*cannot be properly regulated by Member States/regions and/or local authorities acting alone*". Inoltre, secondo il CdR, la proposta avrebbe un valore aggiunto non indifferente, poiché "*a number of benefits which contribute to closing the gap between EU regions and to providing reliable information used to devise health policies geared to local needs*" (punto 27).

[255] Parere del CESE del 26 settembre 2022, punto 1.7.

[256] Parere del CdR dell'8 febbraio 2023.

[257] Per la verità, nel report di fine novembre 2023, il Parlamento europeo ha recepito alcune delle proposte avanzate dal CdR. In particolare, relativamente al coinvolgimento delle autorità locali e regionali nell'assicurare la messa a disposizione delle categorie prioritarie per l'uso primario (art. 4, par. 3, EHDS), nonché riguardo al compito delle autorità di sanità digitale di collaborare non solo a livello sovranazionale, ma anche a livello locale e regionale per lo

elettronici, il Consiglio propone di subordinare la facoltà della Commissione di modificare la lista di dati sanitari contenuti all'art. 14 EHDS a una preventiva valutazione dei bisogni effettivi degli Stati membri [258]. Inoltre, suggerisce di eliminare l'articolo dedicato ai servizi di telemedicina nell'ambito dell'assistenza sanitaria transfrontaliera [259]. In riferimento all'uso secondario dei dati sanitari, tra le altre cose, il Consiglio propone di consentire agli Stati di integrare l'elenco delle finalità per cui tale uso è vietato [260], ritenendo non appropriato che l'Unione introduca delle regole riguardanti l'ordine pubblico e la moralità. Questi aspetti, infatti, rappresentano "*a question of values*" di cui devono poter occuparsi unicamente gli Stati membri [261].

Il Consiglio si è inoltre fatto portatore delle istanze nazionali proponendo una serie di modifiche concernenti la governance dello EHDS e i poteri normativi della Commissione. Per quanto riguarda il primo profilo, viene introdotta la copresidenza nel comitato dello EHDS, composta dalla Commissione e da uno dei rappresentanti degli Stati membri per l'uso primario e secondario dei dati [262]. È prevista anche la sostituzione del gruppo di controllo congiunto con due gruppi direttivi (*steering groups*) per le infrastrutture transfrontaliere MyHealth@EU e HealthData@EU, i quali dovranno includere i rappresentanti dei punti di contatto nazionali [263].

Per quanto riguarda il secondo profilo, il Consiglio suggerisce non solo di sostituire la maggior parte degli atti delegati con atti di esecuzione per introdurre prescrizioni relativamente a temi specifici (ad es. la registrazione dei dati sanitari elettronici e il meccanismo interoperabile e transfrontaliero di

---

sviluppo del formato europeo di scambio e per assicurare l'interoperabilità, la portabilità e la sicurezza dei dati (art. 10, par. 2, lett. h) e m), EHDS). Più in generale, emerge come le principali modifiche proposte dal Parlamento europeo alla proposta della Commissione siano orientate a rafforzare la posizione giuridica delle persone fisiche rispetto all'uso primario e secondario dei loro dati sanitari elettronici.

[258] Art. 5, par. 2, lett. b), EHDS (*general approach* del Consiglio). Nelle proposte del CdR si suggeriva di aggiungere un sottoparagrafo specifico tra i criteri che la Commissione è tenuta a soddisfare nell'elaborazione di atti delegati modificativi della lista di categorie prioritarie di dati (art. 5, par. 2, lett. d). Secondo il CdR, infatti, "*[t]he priorities of new categories must be guided by real needs in the Member States. In many countries, the regional and local level is responsible for healthcare and must be involved in the prioritisation*".

[259] A questo proposito, anche il CdR, in maniera forse meno drastica, aveva proposto di specificare che fossero gli Stati membri a essere incaricati dell'offerta di servizi di telemedicina e non le autorità di sanità digitale, le quali devono limitarsi a favorirne l'offerta a livello nazionale (art. 10, par. 2, lett. k).

[260] Art. 35, par. 3, lett. ba) e f), EHDS (*general approach* del Consiglio).

[261] Modifiche proposte nel parere del CdR all'art. 35, par. 3, EHDS.

[262] Art. 64, par. 1a, EHDS (*general approach* del Consiglio).

[263] Art. 66 EHDS (*general approach* del Consiglio).

identificazione e autenticazione) [264], ma anche di passare dalla procedura di consultazione a quella d'esame per l'adozione degli stessi [265]. Queste modifiche risultano essere particolarmente significative dal momento che un numero maggiore di atti di esecuzione a discapito di quelli delegati testimonia la volontà e l'esigenza di attribuire ai governi nazionali, tramite i c.d. comitati [266], un maggiore controllo sull'operato della Commissione [267].

Controllo che potrà essere anche particolarmente incisivo se si considera la scelta della procedura d'esame [268], invece che di quella consultiva [269]. Nella procedura d'esame, infatti, il comitato è chiamato a pronunciare, con voto a maggioranza qualificata, un parere che vincola l'attività della Commissione. In caso di parere positivo, è possibile procedere all'adozione dell'atto di esecuzione [270]. Al contrario, in caso di parere negativo, l'atto non può essere adottato [271].

Infine, è significativo osservare che non sono state avanzate proposte di modifica alla base giuridica scelta dalla Commissione, neppure da parte del Consiglio, che in passato ha invece svolto un ruolo determinante nel definire il fondamento costituzionale di alcuni atti dell'Unione. Come ricordato in

---

[264] Rispettivamente, artt. 2a, par. 3, e 9, par. 2, EHDS (*general approach* del Consiglio).

[265] Art. 68, par. 2, EHDS (*general approach* del Consiglio).

[266] Cfr. artt. 4 e 5 regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio del 16 febbraio 2011 che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione.

[267] Sulla distinzione tra gli artt. 290 e 291 TFUE, cfr. M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019, p. 1917 ss.; P. CRAIG, G. DE BÚRCA, *op. cit*., 2020, p. 154. Sulla progressiva prevalenza del metodo intergovernativo rispetto a quello comunitario, si veda L.S. ROSSI, *A New Revision of the EU Treaties After Lisbon?*, in L.S. ROSSI, F. CASOLARI, *op. cit*., 2014, p. 5 e U. VILLANI, *Metodo comunitario e metodo intergovernativo nell'attuale fase dell'Unione europea*, in *SIE*, 2019, vol. 2, p. 260.

[268] Art. 5 regolamento (UE) n. 182/2011.

[269] Art. 4 regolamento (UE) n. 182/2011. Secondo tale procedura, prima dell'adozione del testo finale della misura di esecuzione, la Commissione deve tenere in massima considerazione le opinioni emerse nel corso dell'esame effettuato dal comitato o, eventualmente, il parere espresso a maggioranza semplice dallo stesso.

[270] Nell'ulteriore ipotesi in cui il comitato non riesca a esprimere un parere, la Commissione può adottare l'atto di esecuzione a condizione che non riguardi materie sensibili (ad es. la protezione della salute umana), se l'atto di base non glielo vieta o se la maggioranza semplice del comitato non è contraria.

[271] Si ricordi che, tuttavia, anche nell'ipotesi di un parere negativo del comitato, la Commissione può sottoporre al comitato un nuovo progetto di atto entro due mesi dalla sua bocciatura o, eventualmente, ripresentare lo stesso progetto a un comitato di appello. Qualora quest'ultimo esprima parere positivo a maggioranza qualificata, la Commissione potrà adottare l'atto.

precedenza [272], nel corso dell'iter legislativo che ha condotto all'adozione della direttiva 2011/24/UE, è stato proprio il Consiglio a insistere, con successo, affinché la base giuridica della direttiva comprendesse non soltanto l'art. 114 TFUE, come volevano la Commissione e il Parlamento europeo, ma anche l'art. 168 TFUE.

5. Riflessioni conclusive

L'uso flessibile delle disposizioni di diritto primario dell'Unione caratterizza il processo di integrazione europea nel settore della sanità pubblica sin dalle origini. L'inserimento, con il Trattato di Maastricht, di una base giuridica "debole" per questo settore ha stimolato la creatività delle istituzioni europee, le quali hanno fatto e continuano a fare ricorso a strumenti alternativi, come le raccomandazioni fornite nell'ambito del Semestre europeo, la politica fiscale e l'adozione di atti fondati su basi giuridiche "forti" per poter esercitare un'influenza materiale – diretta o indiretta – su gran parte delle decisioni in campo sanitario [273], tra cui quelle relative alle condizioni a cui i cittadini possono accedere alla prevenzione sanitaria e ottenere cure mediche. Tali condizioni, invece che essere "stabilite dalle legislazioni e prassi nazionali" [274], vengono progressivamente "influenzate da misure di armonizzazione e coordinamento adottate a livello sovranazionale" [275]. Ciò avviene non solo per far fronte a situazioni emergenziali [276], ma anche per gestire situazioni ordinarie, che non presentano necessariamente carattere transfrontaliero [277].

---

[272] In particolare, v. sezione 3.2.

[273] L. BUSATTA, *La salute sostenibile. La complessa determinazione del diritto di accedere alle prestazioni sanitarie*, Giappichelli, Torino, 2018, pp. 140 e 241. Per quanto riguarda la distinzione tra l'incidenza diretta e indiretta dell'azione dell'Unione sulle politiche sanitarie nazionali, v. F.A. CANCILLA, *Servizi del welfare e diritti sociali nella prospettiva dell'integrazione europea*, Giuffrè, Milano, 2009.

[274] Art. 35 della Carta.

[275] G. DI FEDERICO, *Unione europea della salute, emergenze e professioni critiche: verso una disciplina ad hoc per gli operatori sanitari?*, in *Eurojus*, 2023, vol. 4, p. 162.

[276] Sull'interpretazione flessibile del principio di attribuzione in contesti emergenziali, cfr. F. CASOLARI, *The EU Approach towards Disaster Management. A Critical Appraisal in the Light of the Action Put in Place to Face the COVID-19 Pandemic*, in *YIDL*, 2023, vol. 4, n. 1, p. 53.

[277] Un discorso analogo può essere fatto anche in riferimento al regolamento (UE) 2021/2282 sulla valutazione delle tecnologie sanitarie, dalla cui analisi si evince come l'intervento dell'Unione finisca per spingersi oltre i confini definiti dai Trattati. Per un approfondimento sul punto, si permetta il rinvio a A. FIORENTINI, *Salute digitale nell'Unione Europea: tra innovazione ed equo accesso all'assistenza sanitaria*, in V. SALVATORE (a cura di), *Digitalizzazione,*

Nel presente capitolo abbiamo evidenziato come lo EHDS rappresenti un ulteriore esempio di legislazione indiretta che consente all'Unione di realizzare un'integrazione più profonda, forzando i limiti costituzionali in ambito sanitario tramite il grimaldello non più solo del mercato interno, ma anche della protezione/libera circolazione dei dati personali. L'art. 16, par. 2, TFUE, in particolare, si aggiunge ai fondamenti normativi che compongono la c.d. "*web of competence*" [278], ossia l'insieme di basi giuridiche, diverse dall'art. 168 TFUE, che permette all'Unione di intervenire in ambito sanitario.

Benché lo EHDS non privi totalmente gli Stati membri della loro autonomia nel decidere dell'organizzazione e del finanziamento dei servizi di assistenza sanitaria [279], tale strumento normativo, unitamente alla leva finanziaria, richiede un'organizzazione e una digitalizzazione dei sistemi sanitari nazionali che è lungi dal potersi dire compiuta specialmente in alcuni Stati membri, imponendo loro un ripensamento significativo delle scelte operate in questo settore. In altre parole, da un lato, la digitalizzazione diventa una condizione per ottenere i finanziamenti del dispositivo di ripresa e resilienza. Dall'altro, una volta avviato questo inevitabile processo di digitalizzazione, le regole comuni per il funzionamento dell'ecosistema digitale sono quelle stabilite dall'Unione.

Pur se vantaggioso in termini di efficienza normativa, l'accentramento che si sta verificando – a Trattati invariati – nel settore sanitario solleva numerosi profili problematici. Il ricorso a basi giuridiche diverse da quella della salute per l'adozione di atti come lo EHDS compromette la legittimità dell'azione dell'Unione [280], in quanto, tra le altre cose, non permette di coinvolgere gli attori istituzionali che hanno la tutela della salute quale obiettivo principale [281]. Inoltre, come ampiamente discusso in questa sede, tale approccio

---

intelligenza artificiale e tutela della salute nell'Unione europea, Giappichelli, Torino, 2023, pp. 123-137.

[278] K.P. PURNHAGEN et al., *More Competences than You Knew?: The Web of Health Competence for European Union Action in Response to the COVID-19 Outbreak*, in *Eur. J. Risk Regul*., 2020, vol. 11, n. 2, p. 297. In particolare, oltre agli artt. 114 e 16, par. 2, TFUE, la "*web of competence*" sarebbe formata dagli artt. 122, 153, 173, 175 e 196. Cfr. V. DELHOMME, T. HERVEY, *op. cit.*, 2022, pp. 54-56; M. FRISCHHUT, *op. cit*., p. 16.

[279] Considerando 20 EHDS.

[280] Come sottolineato da Weatherill, il rispetto del principio di attribuzione e dei limiti all'armonizzazione è essenziale in quanto "*the EU's formal legitimacy is rooted in its Treaties, which were duly authorized by approved constitutional procedures in all Member States*" (p. 847). Forzare le competenze dell'Unione danneggia la sua legittimità dal momento che "*under-explained centralization aggravates mistrust*" (p. 854). Cfr. S. WEATHERILL, *op. cit*., 2011, pp. 827-864.

[281] A. DE RUIJTER, E. BROOKS, *The European Health Union: Strengthening the EU's Health Powers?*, in *Eurohealth*, 2022, vol. 28, n. 3, p. 49: "*When in the EU laws are adopted based on other functional legislative bases, such as the internal market, environment or agriculture, political representation is usually led by institutional actors in that particular field of*

costituisce una minaccia per l'esistenza stessa dell'Unione come Unione di diritto che opera nel rispetto dei limiti posti dai Trattati.

Di fronte a tali criticità, gli Stati membri, diversamente dal passato [282], non si sono opposti alla direzione impressa dall'Unione al processo di integrazione in questo settore né durante la fase di consultazione pubblica precedente alla proposta della Commissione né tramite l'invio di pareri da parte dei parlamenti nazionali. Questa attitudine a non rivendicare, o rivendicare con una certa "timidezza", le proprie prerogative, avallando – almeno per il momento [283] – gli obiettivi strategici perseguiti dall'Unione e gli strumenti scelti per realizzarli, fa presumere l'esistenza di un consenso (tacito) generalizzato a livello nazionale rispetto alle politiche poste in essere dall'Unione, anche qualora queste vadano a limitare le loro prerogative.

---

policy […] Health policy made without health representatives is unlikely to account for the core rights and values of European health systems".

[282] Si veda l'esempio citato nella sezione 2.1 sulla direttiva Bolkestein. Inoltre, con riferimento agli strumenti disponibili successivamente all'adozione dell'atto (v. nota successiva), in passato era più frequente che gli Stati membri, specialmente Germania e Regno Unito, impugnassero *ex* art. 263 TFUE gli atti dell'Unione per violazione dei principi di attribuzione, sussidiarietà e proporzionalità (cfr. R. SCHÜTZE, *op. cit*., 2021, pp. 262-263).

[283] Una volta adottato, l'atto potrebbe essere oggetto di impugnazione davanti alla Corte in sede di sindacato di validità nell'ambito dell'impugnazione diretta (art. 263 TFUE) o del rinvio pregiudiziale (art. 267 TFUE). Con specifico riguardo al principio di sussidiarietà, gli Stati membri possono impugnare un atto legislativo dell'Unione sia per la violazione del principio in quanto tale (sentenza della Corte del 4 maggio 2016, causa C-358/14, *Repubblica di Polonia c. Parlamento e Consiglio*, ECLI:EU:C:2016:323, punti 112 ss.) sia per la violazione degli obblighi procedurali di cui al Protocollo n. 2. Ai sensi dell'art. 8 Protocollo n. 2, infatti, ciascuno Stato membro per conto del proprio Parlamento, e il CdR in caso di un atto legislativo la cui adozione richiede la sua consultazione, può avviare davanti alla Corte un'azione di annullamento *ex* art. 263 TFUE, deducendo la violazione del principio di sussidiarietà. Tale azione è possibile anche se, in precedenza, non è stato presentato un parere motivato negativo in punto di sussidiarietà (P. MENGOZZI, *Commento all'articolo 12 TUE*, in A. TIZZANO (a cura di), *op. cit*., 2014, p. 114; E. CANNIZZARO, *op. cit.*, 2022, p. 290). Detto ciò, nei due mesi successivi all'adozione dello EHDS non è stata promossa alcuna azione di annullamento. Tale esito appare coerente con le perplessità espresse da tempo in dottrina circa le concrete possibilità di successo di ricorsi di questo tipo da parte degli Stati membri, alla luce dell'ampio margine di discrezionalità che la Corte di giustizia riconosce al legislatore dell'Unione sia nella valutazione della necessità e del valore aggiunto dell'intervento sovranazionale, sia nella determinazione della sua proporzionalità, in particolare quando sono in gioco scelte di natura politica, economica o sociale (cfr. J. VAN DE GRONDEN, M. VEENBRINK, *op. cit*., 2024, pp. 276-277).

Capitolo 2
La dimensione economica e sociale dello spazio europeo dei dati sanitari: potenzialità e ostacoli alla sua realizzazione

"*Lo spazio europeo dei dati sanitari rappresenta un elemento centrale dell'Unione europea della salute e una pietra miliare nella trasformazione digitale dell'UE. È uno dei pochi atti legislativi dell'UE in cui creiamo qualcosa di completamente nuovo a livello europeo*".

(Sokol, 2023) [1]

Sommario: 1. Premessa. – 2. Lo spazio europeo dei dati sanitari come spazio di creazione di valore economico nel mercato unico digitale. – 2.1. I rapporti con i regolamenti della Strategia europea per i dati: DGA e DA. – 2.2. L'economia dei dati: accessibilità, circolazione e concorrenza. – 3. Lo spazio europeo dei dati sanitari come naturale sviluppo dello spazio europeo per la ricerca. – 3.1. Le prime esperienze in materia di ricerca scientifica tra collaborazione e integrazione. – 3.2. Il valore aggiunto dello spazio europeo dei dati sanitari. – 4. Lo spazio europeo dei dati sanitari come strumento di attuazione della Carta dei diritti fondamentali. – 4.1. Il diritto fondamentale alla salute. – 4.2. Il diritto fondamentale alla protezione dei dati personali. – 5. Gli ostacoli alla piena realizzazione della dimensione economica e sociale dello spazio europeo dei dati sanitari. – 5.1. L'uso primario dei dati sanitari. – 5.2. L'uso secondario dei dati sanitari. – 5.3. Il cuore della questione: quale bilanciamento tra i diritti e gli interessi in gioco? – 6. Riflessioni conclusive.

1. Premessa

Nel capitolo precedente abbiamo esaminato come la decisione di fondare lo EHDS sugli artt. 114 e 16, par. 2, TFUE sia stata essenzialmente motivata dalla necessità di stabilire regole comuni in un settore, quello sanitario, in cui

[1] Dalla dichiarazione di Tomislav Sokol, correlatore della commissione per l'ambiente e la sanità pubblica, durante la seduta plenaria del Parlamento europeo del 12 dicembre 2023.

l'Unione gode di competenze limitate. Questa scelta non è certamente una novità nel panorama europeo, dove basi giuridiche "forti", soprattutto quella del mercato interno, vengono utilizzate per allargare le strette maglie del sistema di competenze previsto dai Trattati. Il fondamento costituzionale dello EHDS riflette anche un'ulteriore dinamica tipica del processo di integrazione europeo, ossia quella di perseguire obiettivi di natura economica e, al tempo stesso, di carattere sociale [2]. L'impossibilità di tracciare una netta distinzione tra i due è resa plasticamente dalla struttura stessa dello EHDS che si articola in due parti principali, entrambe finalizzate al raggiungimento di molteplici obiettivi, sinteticamente definiti dall'art. 1 EHDS.

Nella prima parte, dedicata all'uso primario dei dati sanitari elettronici [3], l'attenzione è posta sul potenziamento dei diritti delle persone fisiche riguardo al trattamento dei propri dati, sugli obblighi dei professionisti sanitari di garantire la continuità e la qualità delle cure sanitarie, e sull'interoperabilità dei prodotti di sanità digitale (ad es. le cartelle cliniche elettroniche e le applicazioni per il benessere) all'interno del mercato unico. L'accesso sicuro e tempestivo ai dati sanitari da parte delle persone fisiche e dei fornitori di assistenza sanitaria dovrebbe permettere, tra le altre cose, di garantire agli individui il controllo sui propri dati, eliminare le inefficienze nell'erogazione delle cure e prevenire errori medici.

Nella seconda parte, che riguarda l'uso secondario dei dati sanitari [4], vengono dettagliate e sviluppate le modalità di implementazione del regime derogatorio previsto dall'art. 9, par. 2, GDPR per l'uso dei dati relativi alla salute [5]. Queste disposizioni sono motivate dalla consapevolezza che la condivisione e il riutilizzo dei dati sanitari comportano benefici anche per chi non è direttamente coinvolto nella raccolta dei dati, ossia per coloro le cui attività di utilizzo secondario (ad es. ricerca scientifica e innovazione) sono suscettibili di generare vantaggi ulteriori sia in termini economici (ad es. l'abbattimento dei costi dei servizi sanitari) sia in termini di benessere sociale (ad es.

---

[2] Come affermato nell'introduzione al presente lavoro, il termine "sociale" viene qui utilizzato in senso ampio, riferendosi alla dimensione sociale dell'Unione risultante dalle disposizioni dei Trattati concernenti i valori, gli obiettivi (artt. 2 e 3 TUE), ma anche dalle clausole trasversali (artt. 8-13 TFUE) e da alcuni obiettivi specifici (ad es. art. 168 TFUE), nonché dall'incorporazione della Carta tra le norme di diritto primario (art. 6, par. 1, TFUE). Cfr. K. LÖRCHER, *Social Competences*, in N. BRUUN, K. LÖRCHER, I. SCHÖMANN (eds.), *The Lisbon Treaty and Social Europe*, Hart Publishing, Oxford, 2012, p. 165 ss.

[3] Capi II e III EHDS.

[4] Capo IV EHDS.

[5] Per un commento alla suddetta disposizione, si rinvia all'analisi M. TZANOU, *The GDPR and (Big) Health Data: Assessing the EU Legislator's Choices*, in M. TZANOU (eds.), *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Response*, Routledge, London and New York, 2021, p. 18 ss.

l'efficacia e la qualità delle cure, nonché la prevenzione e la gestione delle emergenze sanitarie).

Come si evince dalla struttura dello EHDS, ognuna delle parti che lo compone persegue obiettivi tanto di natura economica, quanto di natura sociale, la cui realizzazione è strettamente interconnessa per via del nesso di funzionalità sussistente tra gli stessi [6]. Nello specifico, è possibile notare come il perseguimento degli obiettivi economici si configura, in ultima analisi, come strumentale alla realizzazione di quelli sociali. La libera circolazione dei dati sanitari e delle cartelle cliniche elettroniche all'interno del mercato unico digitale, ad esempio, non è fine a sé stessa, ma contribuisce a garantire la continuità e la qualità dell'assistenza per le persone che esercitano il diritto alla mobilità nell'Unione [7]. Allo stesso modo, la promozione dell'uso e della condivisione dei dati sanitari aumenta le opportunità di svolgere attività di ricerca scientifica, contribuendo al miglioramento del benessere complessivo.

Nelle pagine seguenti analizzeremo la duplice dimensione dello EHDS, prendendo in esame, in primo luogo, il suo contributo al raggiungimento degli obiettivi di natura economica, per poi soffermarci su quelli di carattere

[6] D'altronde, sin dal Trattato di Lisbona, queste due dimensioni – economica e sociale – costituiscono elementi strutturali del modello economico dell'Unione, definito come "un'economia sociale di mercato fortemente competitiva" (art. 3 TUE). Si tratta di un'espressione che si riferisce alla teoria economica sviluppata dalla scuola di Friburgo e che implica il tentativo di conciliare la logica concorrenziale con finalità sociali e solidaristiche, in un'ottica di coesistenza e complementarità tra le esigenze del mercato e quelle della coesione sociale. La tensione insita in tale definizione è stata oggetto di un ampio dibattito dottrinale: se da un lato essa riflette un compromesso costituzionale volto a temperare l'orientamento neoliberale del processo di integrazione europea, dall'altro lascia emergere una costante difficoltà nel garantire un equilibrio effettivo tra le due anime del progetto europeo. Per un approfondimento sul tema, cfr. E. MUIR, *Drawing Positive Lessons From the Presence of 'The Social' Outside of EU Social Policy* Stricto Sensu, in *Eur. Const. Law Rev.*, 2018, vol. 14, n. 1, p. 79; S. GARBEN, *The Constitutional (Im)balance between "the Market" and "the Social" in the European Union*, in *Eur. Const. Law Rev.*, 2017, n. 1, p. 28; F. DE WITTE, *EU Law, Politics, and the Social Question*, in *Ger. Law J.*, 2013, vol. 14, n. 5, p. 608; P. DE PASQUALE, *L'economia sociale di mercato nell'Unione europea*, in *Studi sull'integrazione europea* 2014, vol. 2, pp. 265-278; G.L. TOSATO, *Appunti in tema di economia sociale di mercato*, in *Scritti in onore di Giuseppe Tesauro*, 2014, vol. 2, p. 2509; G. CONTALDI, *Il significato attuale dell'economia sociale di mercato nell'ordinamento dell'Unione europea*, in *Ordine internazionale e diritti umani*, 2018, n. 5, p. 544. Sul versante più critico, v. anche; F. COSTAMAGNA, *The Internal Market and the Welfare State: Anything New after Lisbon?*, in M. TRYBUS, L. RUBINI (eds.), *The Treaty of Lisbon and the Future of European Law and Policy*, Edward Elgar, Cheltenham, 2012, pp. 381-397.

[7] Art. 3, par. 2, TUE e artt. 20, par. 2, lett. a) e 21, par. 1, TFUE. Con riferimento alla possibilità che le norme sull'uso primario possano contribuire in modo significativo alla libera circolazione dei pazienti nell'Unione, si rinvia ai rilievi critici effettuati nella sezione 3.1 del capitolo 1.

sociale [8]. In particolare, dopo aver calato lo EHDS nel più ampio contesto, normativo e strategico, del mercato unico digitale (sezione 2), evidenzieremo il ruolo che lo stesso riveste nel promuovere e sostenere la ricerca scientifica (sezione 3), e nell'attuare alcuni dei diritti enunciati dalla Carta, come il diritto alla salute e alla protezione dei dati personali (sezione 4). Concluderemo l'analisi mettendo in luce i fattori che potrebbero compromettere la piena realizzazione di tali obiettivi, con particolare riferimento all'assenza o all'insufficiente coordinamento con altri atti di diritto derivato, nonché al delicato bilanciamento tra i diversi diritti e interessi coinvolti nell'interpretazione e applicazione dello EHDS (sezione 5).

2. Lo spazio europeo dei dati sanitari come spazio di creazione di valore economico nel mercato unico digitale

La creazione di un mercato unico digitale rappresenta un obiettivo prioritario per l'Unione europea sin dalla Commissione presieduta da José Barroso [9]. Durante il suo secondo mandato, il presidente portoghese ha sottolineato l'importanza di costruire un mercato unico digitale, garantendo e promuovendo un accesso rapido a Internet per tutti, un elevato livello di sicurezza e privacy, la regolamentazione dei dati e dell'accesso ai contenuti online, nonché la digitalizzazione della pubblica amministrazione [10]. Questa priorità è

[8] A livello metodologico, come anticipato nell'introduzione del presente lavoro, le considerazioni espresse, soprattutto nelle sezioni 2 e 3, – si fonderanno sull'analisi di strumenti di *soft law*. Com'è noto, seppur privi di forza giuridica vincolante, questi strumenti possono comunque produrre effetti giuridici indiretti (cfr. L. SENDEN, *Soft law in European Community Law*, Oxford Portland, Hart Publishing, 2004, p. 112), contribuendo, *inter alia*, a migliorare la comprensione dell'evoluzione dell'azione dell'Unione in ambiti specifici, come il mercato interno e, in particolare, la ricerca.

[9] Per una ricostruzione dettagliata e completa dell'evoluzione del mercato unico digitale nell'ordinamento giuridico europeo, si rimanda all'analisi condotta da F. FERRI, *Il bilanciamento tra diritti fondamentali nel mercato unico digitale*, Giappichelli, Torino, 2022, pp. 25-84. Sul tema si veda anche F. ROSSI DAL POZZO, I. ANRÒ, *Il Mercato Unico Digitale: tra antichi problemi e nuove sfide*, in *Eurojus*, 2025.

[10] Comunicazione della Commissione, Europa 2020: Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 final, del 3 marzo 2010. Vedi anche Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, L'Atto per il mercato unico II. Insieme per una nuova crescita, COM(2012) 573 final, del 3 ottobre 2012; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un quadro coerente per rafforzare la fiducia nel mercato unico digitale del commercio elettronico e dei servizi online, COM(2011) 942 final, dell'1 novembre

stata condivisa anche dalla Commissione Juncker, che nel 2015 ha presentato la nuova strategia per il mercato unico digitale [11]. In questa occasione, il concetto di "mercato unico digitale" è stato definito quale "mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui […] persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali" [12].

Nel contesto delle iniziative volte a promuovere il buon funzionamento del mercato unico digitale, la digitalizzazione del settore sanitario emerge come un fattore chiave per migliorare l'accessibilità e la qualità dell'assistenza

---

2011; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Verso un atto per il mercato unico. Per un'economia sociale di mercato altamente competitiva: 50 proposte per lavorare, intraprendere e commerciare insieme in modo più adeguato, COM(2010) 608 final, del 27 ottobre 2010; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un'agenda digitale europea, COM(2010) 245 final, del 19 maggio 2010. Al lavoro della Commissione Barroso, si affianca anche quello del Parlamento che adotta una serie di risoluzioni, tra cui le risoluzioni del 4 luglio 2013 sul completamento del mercato unico digitale (2013/2655(RSP)); del 20 aprile 2012 sull'eGovernment come elemento trainante di un mercato unico digitale europeo (2011/2178(INI)); del 6 aprile 2011 sulla governance e il partenariato nel mercato unico (2010/2289(INI)), sul mercato unico per gli europei (2010/2278(INI)) e sul mercato unico per le imprese e la crescita (2010/2277(INI)); del 20 maggio 2010 sulla creazione di un mercato unico per i consumatori e i cittadini (2010/2011(INI)).

[11] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia per il mercato unico digitale in Europa, COM(2015) 192 final, del 6 maggio 2015. Così come nel periodo precedente, anche in quello che va dal 2014 al 2019 il Parlamento europeo ha giocato un ruolo centrale nel contribuire alla costruzione del mercato unico digitale, adottando atti legislativi iniziati nella precedente legislatura (ad es. il GDPR) o dando impulso all'adozione di normative strumentali per il buon funzionamento del mercato unico digitale (ad es. il regolamento (UE) 2018/1724 sullo sportello unico digitale). Cfr. G. DI FEDERICO, *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. DI FEDERICO, *Alla (ri)scoperta del Parlamento europeo. 1979-2019*, Giappichelli, Torino, 2021, p. 73 ss.

[12] COM(2015) 192 final, p. 3. In dottrina, il mercato unico digitale viene definito come "*species* del *genus* mercato interno" (B. NASCIMBENE, *Il mercato unico digitale è una nuova frontiera dell'integrazione europea*, in *Eurojus*, 2025, fasc. 3, p. 108; B. NASCIMBENE, *Il Mercato Unico Digitale quale nuova frontiera dell'integrazione europea. Considerazioni introduttive*, in F. ROSSI DAL POZZO, *Mercato Unico Digitale, dati personali e diritti fondamentali*, in *Eurojus*, 2019, p. 11). Similmente, cfr. D. ADAMSKI, *Lost on the Digital Platform: Europe's Legal Travails with the Digital Single Market*, in *CMLRev*., 2018, vol. 55, p. 719; J. SCOTT MARCUS, G. PETROPOULOS, T. YEUNG, *Contribution to Growth: The European Digital Single Market. Delivering Economic Benefits for Citizens and Businesses*, Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2018.

sanitaria, e per aumentare l'efficacia dei sistemi sanitari nazionali [13]. I benefici associati alla digitalizzazione della sanità sono valutati in termini di efficienza nell'organizzazione dei servizi sanitari, portando a un abbattimento dei costi dovuto all'eliminazione di trattamenti non necessari e al miglioramento nella capacità di programmazione [14]. Specialmente in periodi di crisi, le istituzioni vedono nella digitalizzazione uno strumento per rafforzare l'efficienza e la resilienza dei sistemi sanitari, anche nell'ambito del processo del Semestre europeo [15]. Allo stesso tempo, le innovazioni tecnologiche in ambito sanitario sono considerate un volano per la crescita economica e industriale dell'Unione [16], in grado di aumentare le potenzialità del mercato interno [17], specialmente nella sua versione di mercato interno 2.0 [18].

È (anche) in questa prospettiva che la Commissione ha presentato la propria proposta di regolamento sullo EHDS, che dovrebbe comportare benefici complessivi per i pazienti, i finanziatori e i fornitori di beni e servizi sanitari

---

[13] Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo e al Comitato delle regioni, Piano d'azione Sanità elettronica 2012-2020. Una sanità innovativa per il 21esimo secolo, COM(2012) 736 final, del 6 dicembre 2012, in cui il termine *eHealth* viene utilizzato per indicare "l'uso delle tecnologie dell'informazione e della comunicazione (TIC) nei prodotti, servizi e processi sanitari accompagnato da cambiamenti di ordine organizzativo nei sistemi sanitari e nuove competenze al fine di migliorare la salute dei cittadini, l'efficienza e la produttività in ambito sanitario".

[14] COM(2012) 736 final, p. 4; Comunicazione della Commissione europea, Libro verde sulla sanità mobile ("mHealth"), COM(2014) 219 final, del 10 aprile 2014; Conclusioni del Consiglio su una medicina personalizzata per i pazienti, del 17 dicembre 2015; sulla crisi economica e sull'assistenza sanitaria, del 10 luglio 2014; sul processo di riflessione su sistemi sanitari moderni, adeguati e sostenibili, del 10 dicembre 2013, p. 3.

[15] G. Di Federico, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in E. Al Mureden, C. Bottari (eds.), *La salute del futuro: prospettive e nuove sfide del diritto sanitario*, Bononia University Press, Bologna, 2020, pp. 24-25.

[16] Nella proposta di regolamento sui dati viene riconosciuto espressamente che l'istituzione di spazi comuni europei dei dati "contribuirà a creare un autentico mercato interno dei dati che consentirà la condivisione e l'utilizzo dei dati in tutti i settori" (COM(2022) 68 final, del 23 febbraio 2022, p. 3). Sul punto, v. anche la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Aggiornamento della nuova strategia industriale 2020: costruire un mercato unico più forte per la ripresa dell'Europa, COM(2021) 350 final, del 5 maggio 2021, e la Risoluzione del Parlamento europeo del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale (2020/2266(INI)), punti 254 ss.

[17] M.L. Flear, *Regulating New Technologies: EU Internal Market Law, Risk and Socio-Technical Order*, in M. Cremona (ed.), *New Technologies and EU Law*, OUP, Oxford, 2017, p. 76.

[18] A. Renda, *Single Market 2.0: The European Union as a Platform*, in S. Garben, I. Govaere (eds.), *The Internal Market 2.0*, Hart Publishing, Oxford, 2020, p. 188.

fino a 11 miliardi di euro entro 10 anni nel caso di completa applicazione, a fronte di costi incrementali assai più contenuti [19]. Tali benefici sarebbero generati da cambiamenti provocati dall'applicazione delle norme riguardanti sia l'uso primario (5,5 miliardi di euro) sia l'uso secondario (5,4 miliardi di euro) [20].

Per quanto riguarda l'uso primario, i principali vantaggi economici sarebbero

[19] Documento di lavoro della Commissione, Relazione sulla valutazione d'impatto che accompagna la proposta di regolamento sullo spazio europeo dei dati sanitari elettronici, SWD(2022) 131 final, parte 1/4, pp. 56-57. Ai suddetti benefici economici sono associati costi di infrastrutturazione delle reti e di adeguamento ai requisiti normativi, i quali saranno condivisi sia dall'Unione sia dagli Stati membri e dai diversi portatori di interesse (ad es. produttori di cartelle cliniche elettroniche).

[20] SWD(2022) 131 final, p. 69. Per un'analisi critica della metodologia adottata dalla Commissione per valutare i vantaggi economici derivanti dall'uso primario e secondario dei dati, v. J.S. MARCUS et al., *The European Health Data Space*, Publication for the Committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2022. Con riferimento all'uso primario, lo studio in questione critica la scelta della Commissione di concentrarsi soprattutto sugli effetti derivanti dall'adozione di strumenti di telemedicina, trascurando altri benefici economici, "*including patient benefits from being able to switch doctors and search for higher-quality and lower-priced health services, the benefits of innovation, more market transparency and competition in health services*" (p. 29). Inoltre, secondo Marcus et al., un'adeguata analisi costi-benefici avrebbe dovuto considerare non solo vantaggi monetari, ma anche quelli non monetari dovuti al miglioramento degli esiti sanitari e al conseguente effetto positivo sul benessere dei pazienti (p. 30) Pur confermando il rapporto favorevole costi-benefici della valutazione d'impatto della Commissione, gli A. ritengono che "*the cost savings and benefit indicators for primary use in the Commission's IA are not very relevant*" dal momento che "*[b]etter studies exist with more relevant indicators on patient benefits and improved health outcomes as a result of primary data re-use between health service providers*" (pp. 30-31). Viene inoltre criticata l'assenza di una distinzione tra uso primario a livello nazionale e transfrontaliero, osservando come la maggior parte dei benefici economici derivi in realtà dall'uso nazionale dei dati (p. 31), visto il basso tasso di mobilità dei pazienti per cure sanitarie oltreconfine (cfr. relazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, COM(2022) 210 final, del 12 maggio 2022). Analoghe critiche vengono sollevate per quanto riguarda l'uso secondario dei dati. In particolare, gli autori rilevano che la valutazione d'impatto non considera adeguatamente il "*market failure approach*" dovuto alla presenza di esternalità positive derivanti dalla disponibilità di grandi banche dati sanitarie per un'ampia gamma di possibili attività di innovazione e sviluppo con anche benefici non monetari per il miglioramento della qualità dell'assistenza (pp. 32-33). Anche in questo caso, si sottolinea la mancanza di una distinzione tra uso nazionale e uso transfrontaliero, nonostante tale differenziazione sia rilevante: se per alcune patologie comuni può essere sufficiente un pool di dati nazionale, per altre malattie (ad es. quelle rare) è cruciale poter contare su pool di dati transfrontalieri. Nella valutazione dei vantaggi derivanti dall'uso secondario si sarebbero dunque dovute considerare le economie di scala connesse alle dimensioni dei pool di dati, nonché le economie di scopo derivanti dalla possibilità di combinare dati provenienti da più fonti diversificate (p. 34).

legati alla riduzione dei costi di accesso e condivisione dei dati sanitari, grazie all'adozione di un formato europeo standardizzato per lo scambio delle cartelle cliniche elettroniche e all'operatività dell'infrastruttura transfrontaliera MyHealth@EU [21]. Queste novità mirano a ridurre la duplicazione di esami sulle persone, abbreviare i tempi di diagnosi, ampliare e qualificare le opzioni terapeutiche disponibili, diminuire il rischio di errori medici e superare modelli organizzativi inefficienti in ambito assistenziale. Inoltre, si prevede che tali misure favoriscano l'adozione della medicina personalizzata, migliorino l'efficacia dei programmi di prevenzione, rafforzino la sorveglianza epidemiologica e il monitoraggio della sicurezza e dell'efficacia di farmaci e dispositivi medici. A ciò si aggiunge l'introduzione di uno standard europeo di autocertificazione ed etichettatura per, rispettivamente, le cartelle cliniche elettroniche e le applicazioni per il benessere, che dovrebbe stimolare la concorrenza sul mercato, con conseguente contenimento tendenziale dei prezzi e incentivazione all'introduzione di miglioramenti qualitativi [22].

Con riferimento all'uso secondario dei dati, la valutazione d'impatto della Commissione sullo EHDS si sofferma sui risparmi derivanti dai minori costi di accesso ai dati sanitari per finalità di ricerca, innovazione ed elaborazione delle politiche in ambito sanitario. In particolare, una significativa riduzione dei costi dovrebbe derivare dalla possibilità di sostituire la raccolta dei dati tramite il consenso dei singoli individui coinvolti, con il reperimento di dati da grandi database, utilizzabili sulla base di valutazioni svolte dai comitati etici e dagli organismi responsabili per l'accesso ai dati, previo pagamento di tariffe relativamente modeste e calcolate per la copertura di meri oneri di gestione delle suddette banche dati. Si prevede, inoltre, una maggiore capacità dei programmatori, delle autorità di regolamentazione e degli assicuratori privati di utilizzare questi database per definire strategie sanitarie più trasparenti, eque ed efficaci, nonché per garantire un controllo centralizzato della mobilità transfrontaliera. Infine, l'utilizzo dei *real-world data* dovrebbe consentire lo sviluppo di farmaci innovativi e il perfezionamento o l'ampliamento degli usi terapeutici dei farmaci già sul mercato [23].

---

[21] SWD(2022) 131 final, parte 1/4, pp. 54-55.

[22] Ulteriori vantaggi economici sarebbero derivati se fosse stata mantenuta la norma sulla telemedicina. A questo proposito, nella valutazione d'impatto viene sottolineato che "*[t]elemedicine is not only less expensive to EU patients compared to traditional medicine, but it also requires less time taken for patients at health care. Both effects bring about potential savings in terms of the monetary cost of health care for patients and time taken which is monetised by taking the EU gross average salary as a measure of the value of time*" (SWD(2022) 131 final, parte 2/4, p. 45).

[23] SWD(2022) 131 final, parte 1/4, pp. 55-56.

Nella realizzazione di questi obiettivi di carattere economico, lo EHDS non opera *in vacuo*, ma si inserisce nel solco tracciato dalla Commissione con la Strategia europea per i dati del 2020 [24]. Nelle pagine successive, dopo aver illustrato le principali caratteristiche di tale Strategia, esamineremo alcune disposizioni chiave del regolamento sulla governance dei dati (DGA) [25] e del regolamento sui dati (DA) [26]. Questi strumenti normativi, oltre a essere rilevanti per l'applicazione dello EHDS, consentono di evidenziare l'impegno del legislatore europeo nel massimizzare i benefici economici derivanti dall'uso e dal riuso dei dati nell'Unione (sezione 2.1) [27]. L'analisi condotta in questa sezione offrirà l'opportunità di formulare una serie di considerazioni critiche sul modello regolatorio dell'economia dei dati adottato per sostenere lo sviluppo economico dell'Unione e dei suoi Stati membri (sezione 2.2).

---

[24] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati, COM(2020) 66 final, del 19 febbraio 2020.

[25] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati (DGA). Entrato in vigore il 23 giugno 2022, il DGA è applicabile dal 24 settembre 2023.

[26] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati). Il DA, entrato in vigore l'11 gennaio 2024, sarà applicabile dal 12 settembre 2025.

[27] Esula dall'ambito della presente analisi il c.d. "*digital services act package*", che comprende il regolamento sui servizi digitali (DSA) e quello sui mercati digitali (DMA). Considerare questi regolamenti richiederebbe di affrontare non solo la regolamentazione dei dati, aspetto cruciale per comprendere lo EHDS, ma anche quella dei servizi digitali online offerti agli utenti e, in particolare, i principali attori che operano nello spazio digitale, come le piattaforme online di grandi dimensioni e i *gatekeepers*. Nonostante ciò, alcune brevi considerazioni su questi regolamenti verranno comunque riportate all'interno della sezione 2.2, relativa al modello regolatorio dell'economia dei dati. Per una compiuta analisi dei regolamenti in questione, cfr., *inter alia*, G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2021; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, in *I Post di AISDUE*, 2021, vol. 3, pp. 30-56; G. CAGGIANO, *La proposta di* Digital Service Act *per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post di AISDUE*, 2021, vol. 3, pp. 1-29; S. HEIDEBRECHT, *From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance*, in *JCMS*, 2024, vol. 61, n. 1, p. 215 ss.; M. EIFERT et al., *Taming the Giants: The DMA/DSA Package*, in *CMLRev*., 2021, vol. 58, n. 4, p. 989 ss.

2.1. I rapporti con i regolamenti della Strategia europea per i dati: DGA e DA

Lo EHDS rappresenta soltanto il primo degli spazi comuni europei annunciati dalla Commissione nell'ambito della Strategia europea per i dati [28]. Questa Strategia propone una "visione antropocentrica" [29] della trasformazione digitale in atto, a cui dovrà essere affiancata una più ampia strategia industriale per l'Unione, con l'obiettivo di raggiungere una sovranità digitale europea [30]. Uno dei pilastri portanti della Strategia europea per i dati è la costruzione di un quadro normativo intersettoriale [31], finalizzato a sfruttare appieno le potenzialità dei dati e delle nuove tecnologie all'interno di un mercato unico digitale, dove una "quinta libertà" – quella dei dati – si affianca alle tradizionali libertà di merci, persone, servizi e capitali [32].

Non sorprende, in questo contesto, che l'art. 114 TFUE costituisca la base giuridica predominante delle misure adottate [33], diventando così il fondamento

---

[28] Oltre allo EHDS, è prevista l'istituzione di altri spazi in settori strategici, come l'industria, la mobilità, l'agricoltura, l'energia, il turismo, la finanza e la pubblica amministrazione.

[29] Espressione che allude a un approccio regolatorio volto a subordinare l'uso dei dati e delle tecnologie digitali alla tutela degli individui e dei loro diritti fondamentali, nonché al perseguimento di obiettivi di interesse generale. In questa prospettiva, l'aggettivo "antropocentrico" non implica tanto una limitazione all'uso (anche economico) dei dati, quanto piuttosto l'intento di incanalarne la valorizzazione all'interno di un quadro normativo che assicuri il controllo delle persone fisiche sui propri dati e la conformità ai valori dell'Unione.

[30] Il concetto di sovranità digitale è emerso applicando al settore digitale la c.d. "dottrina dell'autonomia strategica", espressione con cui si allude alla capacità dell'Unione di agire in modo autonomo nei principali settori strategici (cfr. F. CASOLARI, C. BUTTABONI, L. FLORIDI, *The EU Data Act in Context: A Legal Assessment*, in *Int. J. Law Inf. Technol*., 2024, vol. 20, p. 3). Sul tema della sovranità digitale, si rinvia, *ex multis*, a: G. FALKNER et al., *Digital Sovereignty – Rhetoric and reality*, in *JEPP*, 2024, vol. 31, n. 8, pp. 2099-2120; S. HEIDEBRECHT, *op. cit.*, 2024, pp. 205-223.

[31] Gli altri tre pilastri della Strategia sono: i) gli investimenti per il potenziamento delle infrastrutture (ad es. *cloud*) e delle capacità europee per l'interoperabilità dei sistemi informativi; ii) l'impegno a fornire alle persone fisiche maggiore controllo sui propri dati, supportando, tra le altre cose, programmi di alfabetizzazione digitale; iii) la creazione di spazi comuni europei per i dati.

[32] Cfr. 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*, 2024, p. 20, in cui si parla di una "quinta libertà" che riguarda una molteplicità di settori, tra cui i dati, la ricerca e l'innovazione.

[33] Vi sono eccezioni, come ad esempio, il regolamento (UE) 2024/903 del Parlamento europeo e del Consiglio del 13 marzo 2024 che stabilisce misure per un livello elevato di interoperabilità del settore pubblico nell'Unione (regolamento su un'Europa interoperabile), la cui base giuridica è l'art. 172 TFUE sulle reti transeuropee.

costituzionale principale per plasmare la sovranità digitale dell'Unione. Oltre alla scelta della base giuridica, gli atti della Strategia europea per i dati condividono due ulteriori caratteristiche.

In primo luogo, questi strumenti normativi sono accomunati dalla natura di regolamenti che, ai sensi dell'art. 288 TFUE, li rende obbligatori in tutti i loro elementi e direttamente applicabili in ciascuno degli Stati membri [34]. A questo proposito, è significativo il ricorso al termine "*act*" nei titoli dei principali regolamenti adottati nel quadro della Strategia. Una scelta terminologica che, pur non avendo un significato specifico nell'ordinamento dell'Unione, riflette una precisa volontà politico-istituzionale di intervenire in maniera incisiva, con un approccio *top-down* [35]. L'adozione di questa tipologia di atti, identificata come la forma più integrata della legislazione europea [36], mira a ridurre la frammentazione normativa risultante dalla stagione legislativa precedente. In particolare, ci si riferisce alla situazione di frammentazione

[34] R. SCHÜTZE, *European Constitutional Law*, OUP, Oxford, 2021, pp. 164-166.

[35] La tendenza del legislatore europeo a preferire la forma del regolamento, piuttosto che quella della direttiva, è evidente se si pensa agli atti che sono stati recentemente adottati, specialmente in ambito digitale. V., *inter alia*, regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (*Cyber Resilience Act*); regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (*Artificial Intelligence Act*); DA; regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (DSA); regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (DMA); regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio del 13 settembre 2023 che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il regolamento (UE) 2021/694 (*Chips Act*); DGA. Questa tendenza è stata descritta dalla dottrina in termini di *act-ification* (V. PAPAKONSTANTINOU, P. DE HERT, *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, in *TechReg*, 2022 e V. PAPAKONSTANTINOU, *The "Act-ification" of EU Law: The (Long-Overdue) Move Towards "Eponymous" EU Legislation*, in *European Law Blog*, 2021). Per una lettura critica del fenomeno di *act-ification* in ambito sanitario, si consenta il rinvio a A. FIORENTINI, *Salute digitale nell'Unione Europea: tra innovazione ed equo accesso all'assistenza sanitaria*, in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Giappichelli, Torino, 2023, p. 127.

[36] G. GAJA, P. HAY, R.D. ROTUNDA, *Instruments for Legal Integration in the European Community – A Review*, in M. CAPPELLETTI, M. SECCOMBE, J.H. WEILER (eds.), *Integration Techniques and Judicial Process*, De Gruyter, Berlin, 1986, p. 124.

derivante dalla discrezionalità lasciata agli Stati membri nell'applicazione di alcune delle disposizioni del GDPR [37] e della direttiva 2011/24/UE [38].

In secondo luogo, i regolamenti della Strategia europea per i dati si distinguono per un'impostazione che richiama, sotto molteplici profili – definitorio, sostanziale e istituzionale – il GDPR (fenomeno spesso definito come "*GDPR mimesis*") [39]. Ciononostante, essi introducono anche elementi di novità, specialmente per quanto riguarda la presenza di disposizioni volte a promuovere l'uso e la condivisione dei dati. Come anticipato, ci concentreremo sull'analisi del DGA e del DA, con particolare attenzione alle norme di maggiore rilevanza anche per l'applicazione dello EHDS.

Nel DGA, la condivisione dei dati per scopi diversi da quelli iniziali – siano essi commerciali o non commerciali – è favorita tramite l'introduzione di un meccanismo delle richieste di riutilizzo dei dati generati da enti pubblici. Si tratta di dati esclusi dall'ambito di applicazione della direttiva *open data* [40] in quanto protetti per motivi di riservatezza commerciale, riservatezza statistica, protezione dei diritti di proprietà intellettuale di terzi e protezione dei dati personali [41]. A differenza dello EHDS [42], il DGA non impone un obbligo agli enti pubblici di condivisione dei dati. Tuttavia, questi possono concedere o negare l'accesso per il riutilizzo dei dati sulla base di specifiche condizioni [43],

---

[37] Benché tale aspetto verrà affrontato più approfonditamente nel capitolo 4, si anticipa finora che le norme del GDPR che hanno generato maggiore frammentazione sono quelle concernenti la base giuridica del trattamento dei dati sanitari.

[38] Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera. Come analizzato nelle sezioni 3.2 e 4.3 del capitolo 1, le maggiori criticità emerse nell'attuazione degli aspetti digitali di tale direttiva derivano, per l'uso primario dei dati, dalla mancanza di vincolatività delle iniziative promosse nell'ambito della rete volontaria di assistenza sanitaria online, mentre per quanto riguarda l'uso secondario dei dati, dall'assenza di volontà politica nel perseguimento di simili obiettivi. Cfr. il documento di lavoro della Commissione sulla relazione di valutazione di impatto che accompagna la proposta di regolamento sullo spazio europeo dei dati sanitari elettronici, SWD(2022) 131 final, parte 4/4.

[39] V. PAPAKONSTANTINOU, P. DE HERT, *op. cit.*, 2022.

[40] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (direttiva *open data*). Nel confermare il principio *open by design and by default* per i dati in possesso del settore pubblico, tale direttiva amplia l'ambito soggettivo di applicazione dell'intervento precedente (art. 5, par. 2). Per un approfondimento, cfr. S. GOBBATO, *Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese*, in *MediaLaws*, 2020, n. 2, p. 247 ss.; A. FIORENTINI*, Il recepimento della Direttiva Open Data: un punto di svolta per la ricerca in Italia?*, in *Eurojus*, 2021.

[41] Art. 3, par. 1, DGA.

[42] Art. 51 EHDS.

[43] Art. 5 DGA.

eventualmente avvalendosi del supporto di organismi nazionali competenti [44]. In ambito sanitario, tali organismi nazionali potrebbero essere incaricati di gestire le richieste di riutilizzo dei dati sanitari laddove uno Stato membro non abbia designato un ente *ad hoc* che svolga il ruolo proprio degli organismi per l'accesso ai dati sanitari elettronici [45].

Ulteriore elemento di incentivo alla condivisione dei dati nel DGA è rappresentato dalla possibilità per gli Stati membri di stabilire disposizioni organizzative o tecniche e politiche nazionali per permettere e favorire l'altruismo dei dati. Espressione con cui ci si riferisce alla condivisione di dati sulla base del consenso dell'interessato, in caso di dati personali, o dell'autorizzazione del titolare dei dati, in caso di dati non personali, per fini di interesse generale (ad es. assistenza sanitaria e ricerca scientifica) [46]. Per attuare tali pratiche, il DGA prevede che gli Stati membri debbano designare delle organizzazioni per l'altruismo dei dati [47]. Nel settore sanitario, questi soggetti saranno tenuti a rispettare un codice specifico, adottato dalla Commissione con atto delegato, contenente requisiti tecnici e di sicurezza, nonché indicazioni sulle informazioni da fornire agli interessati o ai titolari prima di ottenere il consenso o l'autorizzazione per l'altruismo dei dati [48].

In modo complementare al DGA, il DA stabilisce un quadro normativo armonizzato per la condivisione dei dati generati dall'uso di un prodotto o di un servizio correlato sia nei confronti degli utenti di tale prodotto o servizio che, in situazioni di necessità eccezionali, verso enti pubblici o istituzioni, agenzie o organismi dell'Unione. In particolare, il DA richiede che i prodotti e i servizi in questione siano progettati in modo che i dati generati siano accessibili all'utente per impostazione predefinita [49]. Qualora ciò non sia tecnicamente possibile, il DA – analogamente allo EHDS [50] – impone al titolare di mettere a disposizione dell'utente i dati, senza ritardi e gratuitamente [51], consentendogli altresì di richiedere la loro trasmissione verso soggetti terzi, specificatamente individuati [52].

Come anticipato, l'obbligo del titolare di mettere a disposizione i dati non si esaurisce nei confronti dell'utente, ma si estende, in circostanze straordinarie

---

[44] Art. 7 DGA.

[45] Considerando 64 EHDS.

[46] Artt. 2, n. 16 e 16 DGA.

[47] Artt. 17-21 DGA.

[48] Art. 22 DGA.

[49] Art. 3, par. 1, DA.

[50] Art. 51 EHDS.

[51] Art. 4, par. 1, DA.

[52] Art. 5 DA.

(quali emergenze sanitarie), anche agli enti pubblici e agli organismi dell'Unione [53]. Tuttavia, tale accesso ai dati deve essere considerato come una "*last resort possibility*" [54], utilizzabile solo quando non sia possibile ottenere i dati attraverso altri canali, come quelli previsti dallo EHDS per l'uso secondario. Inoltre, nel caso in cui venga concesso tale accesso, i dati non possono essere resi disponibili per il riutilizzo, ai sensi del DGA o della direttiva *open data* [55], salvo in due ipotesi: i) quando la condivisione avvenga a favore di soggetti o enti senza scopo di lucro che conducano attività di ricerca o analisi scientifiche compatibili con le finalità originarie della richiesta; oppure ii) quando essa avvenga nell'ambito di una missione di interesse pubblico riconosciuta dal diritto dell'Unione o nazionale [56].

Analogamente a quanto previsto per lo EHDS, anche l'attuazione del quadro normativo predisposto dal DGA e dal DA è destinata a generare importanti benefici economici. Per quanto riguarda il DGA, l'istituzione di regole comuni sulla condivisione e sul riutilizzo dei dati nel settore pubblico e, in particolare, in quello sanitario, dovrebbe favorire lo sviluppo di cure migliori e personalizzate, servizi più efficienti e nuovi prodotti basati sui dati, con un risparmio annuale di circa 120 miliardi di euro entro il 2027 [57]. Quanto poi al DA, si stima che l'accesso e lo scambio dei dati generati dai prodotti per l'uso commerciale e per scopi di interesse pubblico dovrebbero comportare benefici economici per il settore sanitario di circa 100 miliardi di euro [58]. Queste cifre sottolineano la centralità strategica dei dati come risorsa economica chiave per l'Unione.

Oltre all'impatto diretto sui settori produttivi, l'ampliamento del volume e della qualità dei dati disponibili a livello europeo contribuirebbe in modo sostanziale al rafforzamento della competitività europea e allo sviluppo di tecnologie innovative, *in primis* l'Intelligenza Artificiale (IA). In questo ambito, un ruolo cruciale sarà svolto dagli spazi comuni europei di dati, come lo EHDS, che dovrebbero facilitare l'accesso non discriminatorio ai dati, così come l'addestramento sicuro, tempestivo, trasparente e affidabile di sistemi di IA su tali set di dati [59]. Ciò in conformità ai valori europei di cui all'art. 2 TUE, elevati a componente essenziale della matrice identitaria dell'Unione

---

[53] Artt. 14-15 e considerando 57-58 DA.

[54] DG SANTE, *Frequently Asked Questions on the European Health Data Space*, 2025, p. 43.

[55] Art. 17, par. 3, DA.

[56] Art. 21 DA.

[57] SWD(2020) 295 final, p. 2.

[58] *Ibid.* p. 68.

[59] Considerando 68 AIA.

dalla giurisprudenza "emergenziale" della Corte sullo Stato di diritto [60].

In questa prospettiva, l'approccio seguito dall'Unione per la piena realizzazione del mercato unico digitale si distingue radicalmente rispetto a quello adottato dagli Stati Uniti (basato sull'autoregolazione) e dalla Cina (caratterizzato da un controllo statale più marcato). Parte della dottrina ha sostenuto la maggiore idoneità, anche nel contesto europeo, di soluzioni basate sull'autoregolazione o sulla co-regolazione [61]. L'Unione, tuttavia, ha scelto consapevolmente un percorso differente, orientato verso una regolazione di tipo "*top-down*", capace – almeno in potenza – di porre al centro la protezione dei valori comuni.

Considerata la rilevanza strategica del mercato europeo dei dati, è ragionevole ipotizzare che attori economici extra-UE – desiderosi di accedervi – dovranno progressivamente adattarsi al modello europeo, così come è già accaduto con il GDPR. In tale contesto, nonostante le incertezze legate all'orientamento della nuova amministrazione statunitense, è lecito attendersi l'emergere, anche per i regolamenti della Strategia europea per i dati, del c.d. *Brussels Effect*, fortunata espressione coniata da Anu Bradford per descrivere la capacità dell'Unione di proiettare i propri standard normativi oltre i propri confini, influenzando così l'evoluzione delle regolazioni globali [62].

2.2. L'economia dei dati: accessibilità, circolazione e concorrenza

Dall'analisi dei principali regolamenti adottati nell'ambito della Strategia europea per i dati emerge un modello regolatorio per l'economia dei dati (*data economy*) che cerca di coniugare l'innovazione e la competitività con la protezione dei diritti individuali, puntando al contempo a contrastare

---

[60] Sentenze della Corte del 16 febbraio 2022, causa C-156/21, *Ungheria c. Parlamento e Consiglio*, ECLI:EU:C:2022:97, punto 127 e causa C-157/21, *Repubblica di Polonia e Ungheria c. Parlamento europeo e Consiglio dell'Unione*, ECLI:EU:C:2022:98, punto 145. Sulla dimensione valoriale dell'AIA, si rinvia all'analisi di F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *DUE*, 2022, vol. 27, n. 2, p. 294 ss.: l'A. individua l'AIA, così come il DMA e il DSA, quali esempi emblematici della tendenza normativa a livello europeo di adottare regolamenti finalizzati a concretizzare i valori fondanti dell'Unione.

[61] Cfr., *inter alia*, G. CONTALDI, *L'approccio regolatorio dell'Unione europea in materia di intelligenza artificiale*, in *Quaderni AISDUE*, 2026, pp. 3-4; M. FINCK, *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy*, in *Eur. Law Rev.*, 2018, vol. 43, n. 1, pp. 47-69.

[62] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, OUP, Oxford, 2020.

l'attuale tendenza verso forme di mercato più concentrate in senso oligopolistico [63]. Questo modello regolatorio si fonda su tre pilastri fondamentali, accomunati dall'obiettivo di aumentare sia il valore dei dati sia la loro effettiva disponibilità.

Il primo pilastro riguarda la promozione dell'accesso ai dati, in particolare a quelli detenuti da enti pubblici, secondo il principio dell'"apertura fin dalla progettazione e per impostazione predefinita" [64]. In tal senso, il DGA rappresenta la prosecuzione – senza soluzione di continuità – di una politica di apertura dei dati avviata con la direttiva 2003/98/CE [65] e poi evoluta con la direttiva *open data*. Il DGA estende la disciplina esistente ai dati soggetti a vincoli di accesso per motivi di riservatezza commerciale, statistica, tutela dei diritti di proprietà intellettuale o protezione dei dati personali. Si inserisce in questa logica anche il regolamento di esecuzione sugli insiemi di dati di elevato valore, che, sulla base delle sei categorie individuate dalla direttiva *open data*, identifica specifici dataset ad alto impatto, generati o detenuti da enti pubblici [66], la cui apertura dovrebbe arricchire la disponibilità di dati negli spazi comuni europei, migliorandone al contempo qualità, interoperabilità e riutilizzabilità su scala transfrontaliera.

Il secondo pilastro è costituito dall'adesione ai principi FAIR [67], che guidano il trattamento e la circolazione dei dati nell'ambito della Strategia. Tali principi impongono che i dati siano: reperibili (*findable*) tramite l'uso di identificatori unici e di metadati altamente descrittivi; accessibili (*accessible*) attraverso il ricorso a protocolli di autenticazione e autorizzazione volti a garantire il rispetto degli obblighi giuridici esistenti; interoperabili (*interoperable*) tramite l'impiego di standard comuni in grado di favorire il flusso dei dati; riutilizzabili (*re-usable*), ossia devono poter essere trattati per finalità diverse da quelle originarie. Il pieno rispetto dei principi FAIR è fondamentale per il funzionamento degli strumenti previsti sia nel DGA che nello EHDS, in particolare con riferimento al riutilizzo dei dati sanitari elettronici per scopi secondari [68].

Il terzo pilastro si fonda su un approccio "solidaristico", volto a contrastare la concentrazione del potere economico e informativo nelle mani di pochi

---

[63] Garante europeo della protezione dei dati (EDPS), *Opinion 3/2020 on the European strategy for data*, p. 2.

[64] Art. 5, par. 2, direttiva (UE) 2019/1024.

[65] Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.

[66] Allegato al regolamento (UE) 2023/2854.

[67] M. WILKINSON et al., *The FAIR Guiding Principles for Scientific Data Management and Stewardship*, in *Scientific Data*, 2016, vol. 3, pp. 1-9.

[68] Considerando 2 DGA e considerando 3 e 85 EHDS.

attori dominanti, secondo il c.d. *Integrated Platform Model*. Tale modello, incarnato dalle grandi piattaforme digitali globali (GAFAM) [69], si basa sull'accumulo e sull'analisi di vasti volumi di dati, che consente loro di trarre esclusivo vantaggio dalla monetizzazione del trattamento dei dati personali [70]. I monopoli e gli oligopoli che ne derivano rappresentano un rischio per la concorrenza [71], oltre che per la protezione dei dati personali [72].

Per prevenire il consolidarsi di tali forme di accentramento del potere, la Strategia europea per i dati propone un modello regolatorio improntato a una logica marcatamente redistributiva [73], con l'obiettivo di garantire una più equa distribuzione del valore economico dei dati tra i diversi attori coinvolti nella *data economy* [74]. Questo approccio si riflette non solo nel DGA e nel DA, ma anche nei regolamenti orizzontali sui mercati e servizi digitali – rispettivamente il *Digital Markets Act* (DMA) [75] e il *Digital Services Act* (DSA) [76] – che mirano a riequilibrare i rapporti di forza tra utenti, imprese e piattaforme, promuovendo un ecosistema digitale più aperto, pluralistico e rispettoso dei diritti.

In particolare, il DMA vieta ai *gatekeepers* [77] di utilizzare i dati raccolti dagli utenti delle loro piattaforme per competere direttamente con questi ultimi,

---

[69] Acronimo utilizzato per riferirsi a Google, Amazon, Facebook (ora Meta) e Microsoft.

[70] SWD(2020) 295 final, pp. 19-20.

[71] Coloro che detengono grandi quantità di dati impediscono l'accesso ad altri tramite strumenti tecnologici ed ottengono così un vantaggio competitivo che altera il libero sviluppo di un mercato concorrenziale, in spregio agli artt. 101 e 102 TFUE. Cfr. A. GALIANO et al., *I dati non personali: la natura e il valore*, in *RIID*, 2020, n. 1, pp. 11-15; G. SCHNEIDER, *Health Data Pools Under European Data Protection and Competition Law. Health as a Digital Business*, Springer, Berlin, 2022, pp. 115-117.

[72] Sulla progressiva interrelazione tra le due branche del diritto, v. P. MANZINI, *Antitrust e privacy: la strana coppia*, in P. MANZINI (a cura di), *I confini dell'antitrust. Diseguaglianze sociali, diritti individuali e concorrenza*, Giappichelli, Torino, 2023, pp. 123-143; A. D'AMICO, *The Boundary between EU Competition Law and the GDPR after* Meta, in *CML-Rev*., 2024, vol. 61, n. 3, pp. 787-804; F. COSTA-CABRAL, O. LYNKSEY, *Family Ties: the Intersection between Data Protection and Competition in EU law*, in *CMLRev*., 2017, vol. 54, n. 1, pp. 12-13; G. BELLITTI, *Big data e abuso di posizione dominante*, in A. CATRICALÀ, C.E. CAZZATO, F. FIMMANÒ, *Diritto antitrust*, Giuffrè, Milano, 2021, pp. 477-479; A. SOLA, *Primi cenni di regolazione europea nell'economia dei dati*, in *MediaLaw*, 2022, vol. 3, pp. 205-208.

[73] SWD(2020) 295 final, pp. 19-20.

[74] Valutazione d'impatto iniziale della Commissione sul DA, Ref. Ares(2021)3527151, del 28 maggio 2021.

[75] Entrato in vigore l'1 novembre 2022, il DMA è applicabile dal 2 maggio 2023.

[76] Il DSA è entrato in vigore a novembre 2022 ed è applicabile da luglio 2023 per le piattaforme molto grandi, mentre da gennaio 2024 per tutti gli altri attori.

[77] Ai sensi del DMA, i *gatekeepers* sono imprese che: i) hanno un impatto significativo sul mercato interno, ii) forniscono un servizio di piattaforma di base che costituisce un punto di accesso importante affinché gli utenti commerciali raggiungano gli utenti finali, e iii)

e proibisce la combinazione dei dati personali degli utenti provenienti da servizi diversi della medesima piattaforma, salvo consenso [78]. Il DSA, invece, introduce obblighi di trasparenza finalizzati a garantire l'accesso, in condizioni specifiche, ai dati raccolti dalle grandi piattaforme online e dai motori di ricerca di dimensioni molto grandi [79]. In questo contesto, tali entità sono tenute, ad esempio, a consentire l'accesso ai dati da parte di ricercatori affiliati a organismi di ricerca, previa autorizzazione del coordinatore dei servizi digitali [80].

Il DGA, a sua volta, impone agli enti pubblici il divieto di stipulare accordi che conferiscano, esplicitamente o implicitamente, un'esclusiva nell'accesso o nel riutilizzo dei dati da essi detenuti, o che ne limitino la disponibilità per altri potenziali riutilizzatori [81]. Questo serve a garantire che i dati di interesse pubblico possano essere condivisi in modo equo e non discriminatorio. Il DA, d'altra parte, riconosce agli utenti diritti di accesso e portabilità rispetto ai dati generati attraverso l'uso di prodotti connessi o servizi correlati, con l'obiettivo di contrastare le dinamiche oligopolistiche tipiche del settore dei servizi di trattamento dei dati (ad es. i servizi di *cloud* ed *edge computing*) [82].

Per garantire tale accesso, il DA impone ai produttori di dispositivi e ai fornitori di servizi l'obbligo di mettere a disposizione i dati raccolti all'utente o, su richiesta di quest'ultimo, a fornitori terzi [83]. L'intento è quello, ancora una volta, di evitare che solamente pochi attori privati (ad es. i *gatekeepers*) possano trarre profitto dall'analisi e dall'elaborazione dei dati di cui dispongono, sviluppando ad esempio farmaci o terapie digitali, a cui possono accedere con più facilità (o in via esclusiva) persone che dispongono di maggiori risorse economiche [84], oppure svolgendo attività che non hanno alcun legame

---

detengono una posizione consolidata e duratura nell'ambito delle proprie attività, o è prevedibile che acquisiscano tale posizione in futuro (artt. 2 e 3, par. 1, DMA).

[78] Artt. 5, par. 2, e 6, par. 2, DMA.

[79] Art. 33 ss. DSA.

[80] Art. 40 e considerando 97 DSA. Sul punto, si veda anche il regolamento delegato della Commissione del 1° luglio 2025 che integra il regolamento delegato (UE) 2025/2050 della Commissione del 10 luglio 2025 che integra il regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio stabilendo le condizioni tecniche e le procedure alle quali i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi devono condividere i dati con ricercatori abilitati.

[81] Art. 4 DGA.

[82] Artt. 4 e 5 DA. Similmente, il DMA richiede che i *gatekeepers* mettano a disposizione degli utenti strumenti efficaci per agevolare l'effettiva portabilità dei dati forniti dall'utente finale o generati mediante l'attività dell'utente finale nell'utilizzo dei servizi di piattaforma di base (art. 6, par. 9, DMA).

[83] Artt. 3-12 DA.

[84] Cfr. E.G. HOWE III, F. ELENBERG, *Ethical Challenges Posed by Big Data*, in *Innov. Clin. Neurosci*., 2020, vol. 17, nn. 10-12, pp. 24-30; J. COLLMANN, S.A. MATEI, *Ethical Reasoning*

con finalità di interesse generale, ma mirano esclusivamente alla massimizzazione dei loro profitti (ad es. strategie di *pricing* personalizzate o pubblicità mirata) [85].

Alla luce di quanto esposto, il modello regolatorio dell'Unione per l'economia dei dati incoraggia l'accessibilità e la circolazione dei dati e punta a ridurre il rischio di posizioni monopolistiche da parte di pochi attori in posizioni dominanti, promuovendo la concorrenza e garantendo un accesso equo ai dati per tutti gli operatori del mercato. Al tempo stesso, tale modello intende anche sostenere l'innovazione attraverso regolamenti che favoriscono l'uso e la condivisione responsabile e sicura dei dati, nel rispetto dei valori dell'Unione.

3. Lo spazio europeo dei dati sanitari come naturale sviluppo dello spazio europeo per la ricerca

Se nella sezione precedente abbiamo insistito sulla dimensione più strettamente economica dello EHDS, il nostro interesse si sposta ora su quella sociale. Un primo elemento utile a orientare questa riflessione è la scelta terminologica del legislatore europeo di parlare di "spazio" anziché di "mercato" dei dati sanitari. Tale opzione lessicale denota l'intenzione di emanciparsi da una prospettiva eminentemente mercantilistica, che rischierebbe di attribuire un peso eccessivo al valore economico dei dati, trascurando invece il loro potenziale contributo al miglioramento di diversi aspetti della via sociale. In altre parole, il termine "spazio" è evocativo di una volontà del legislatore europeo di sottolineare come il processo di integrazione non si limiti a realizzare obiettivi commerciali ed economici, ma comprenda anche finalità di natura sociale [86].

Prima di essere formalmente inclusa nel diritto dell'Unione, la locuzione "spazio europeo", spesso accompagnata da aggettivi specifici come "giuridico" o "giudiziario", descriveva ambiti in cui gli ordinamenti degli Stati e

---

in Big Data: An Exploratory Analysis, Springer, New York, 2016. Per una critica generale alle pratiche di raccolta e sfruttamento dei dati dei consumatori a favore delle classi più agiate, cfr. J.E. COHEN, *Irrational Privacy?*, in *J. Telecomm. & High Tech. L.*, 2012, vol. 10, p. 245.

[85] G. SCHNEIDER, *op. cit.*, 2022, p. 113.

[86] Simili osservazioni sono state compiute con riferimento alla definizione di mercato interno come "*spazio* senza frontiere interne", contenuta all'art. 26, par. 2, TFUE. In particolare, Lenaerts e Nuffel affermano che la scelta di una simile definizione riflette l'intenzione del legislatore europeo di fare in modo che l'integrazione non sia "*confined to economic factors of production*", ma includa "*the whole of life in society*" (K. LENAERTS, P. VAN NUFFEL, *European Union Law*, Thomson Reuters, London, 2011, p. 201).

della Comunità si integravano, formando un sistema unitario con uniforme applicazione. Una volta codificata all'interno dei Trattati istitutivi, questa espressione ha assunto un valore giuridico, oltre che descrittivo, per indicare "aree di comune interesse dell'Unione e degli Stati membri in cui le rispettive sfere tendono a combinarsi stabilmente, offrendo agli interessati una base giuridica per nuove loro situazioni giuridiche soggettive" [87].

Caratterizzati da elementi di federalismo [88], gli "spazi europei" possono essere considerati come manifestazioni tangibili dell'idea di un'"unione più stretta" [89], che fin dalle origini anima il progetto d'integrazione europea. L'obiettivo della loro istituzione è, tra le altre cose, creare degli ambiti di cooperazione e solidarietà basati su rapporti di fiducia reciproca per quanto riguarda il rispetto delle norme e dei valori dell'Unione [90]. Di conseguenza, così

---

[87] M.P. CHITI, A. NATALINI (a cura di), *Lo Spazio amministrativo europeo. Le pubbliche amministrazioni dopo il Trattato di Lisbona*, Il Mulino, Bologna, 2012, pp. 37-38. Gli A. mettono in luce come l'avvio delle discussioni sull'affermarsi di uno Spazio amministrativo europeo abbia coinciso con l'introduzione della moneta unica, ossia il momento in cui la capacità di attuare le politiche europee stava diventando di fondamentale importanza. Era quindi necessario assicurare "una convergenza tra le amministrazioni comunitarie e quelle dei diversi Paesi membri in direzione di una sorta di modello comune europeo". Sul punto, si veda anche C.H. HOFMANN, *Mapping the European Administrative Space*, in *West European Politics*, 2008, vol. 31, n. 4, p. 671; J. TRONDAL, *Administrative Fusion: Less Than a European 'Mega-administration'*, in *J. Eur. Integr.*, 2009, vol. 31, n. 2, pp. 237-260; J. OLSEN, *Towards a European Administrative Space?*, in *J. Eur. Public Policy*, 2003, vol. 10, n. 4, pp. 506-531.

[88] In linea generale, gli "spazi europei" si contraddistinguono per una combinazione di competenza dell'Unione e degli Stati, con un forte coinvolgimento e coordinamento a livello europeo.

[89] Preambolo e art. 1 TUE, e preambolo del TFUE e della Carta.

[90] Questo atteggiamento di fiducia dovrebbe caratterizzare tanto i rapporti tra i cittadini e l'Unione, quanto quelli tra gli Stati membri, i quali dovrebbero poter contare sul fatto "che tutti gli altri Stati membri rispettano il diritto dell'Unione e, più in particolare, i diritti fondamentali riconosciuti da quest'ultimo" (parere 2/13 della Corte del 18 dicembre 2014, ECLI:EU:C:2014:2454, punto 191). In dottrina, sul principio di mutua fiducia, cfr. C. RIZCALLAH, *The Principle of Mutual Trust and the Protection of Fundamental Rights in the Area of Freedom, Security and Justice: A Critical Look at the Court of Justice's Stone-by-Stone Approach*, in *MJECL*, 2023, vol. 30, n. 3, p. 1; L.S. ROSSI, *Fiducia reciproca e mandato d'arresto europeo. Il "salto nel buio" e la rete di protezione*, in *FSJ*, 2021, n. 1, p. 1; F. MAIANI, S. MIGLIORINI, *One Principle to Rule Them All? Anatomy of Mutual Trust in the Law of the Area of Freedom, Security and Justice*, in *CMLRev.*, 2020, vol. 57, n. 1, p. 7; E. REGAN, *The Role of the Principles of Mutual Trust and Mutual Recognition in EU Law,* in *DUE*, 2018, fasc. 2, p. 231; K. LENAERTS, *La vie après l'avis: Exploring the Principle of Mutual (Yet not Blind) Trust*, in *CMLRev*., 2017, vol. 54, p. 813 ss.; S. PRECHAL, *Mutual Trust before the Court of Justice of the European Union*, in *European Papers*, 2017, vol. 2, p. 75; E. PISTOIA, *Lo status del principio di mutua fiducia nell'ordinamento dell'Unione secondo la giurisprudenza della Corte di giustizia. Qual è l'intruso?,* in *FSJ*, 2017, n. 2, p. 26; K. LENAERTS, *The Principle of Mutual Recognition in the Area of Freedom, Security and Justice*, in *DUE*, 2015, fasc. 3, p.

come evidenziato in precedenza relativamente al modello regolatorio della *data economy*, è possibile notare come la regolamentazione di questi spazi si fonda su un modello valoriale o *right-based* [91] che prende le distanze dal paradigma del "fondamentalismo del mercato" [92].

Sebbene nell'ordinamento europeo siano stati istituiti diversi "spazi" [93], merita di richiamare in questa sede lo spazio europeo per la ricerca (SER) [94] poiché rappresenta un'iniziativa che, pur animata da obiettivi di integrazione e cooperazione analoghi a quelli che hanno guidato la creazione dello EHDS, non ha tuttavia raggiunto l'impatto e la diffusione auspicati al momento della sua istituzione. Al contrario, alcune scelte adottate per la realizzazione dello EHDS appaiono, almeno sul piano ideale, particolarmente efficaci.

Per questo motivo, nelle pagine che seguono, dopo un breve *excursus* sulle

---

525; E. BROUWER, D. GERARD (eds.), *Mapping Mutual Trust: Understanding and Framing the Role of Mutual Trust in EU Law*, in *EUI Working Paper MWP*, 2016, p. 59; C. FAVILLI, *Reciproca fiducia, mutuo riconoscimento e libertà di circolazione di rifugiati e richiedenti protezione internazionale nell'Unione europea*, in *Rivista di diritto internazionale*, 2015, vol. 98, n. 3, p. 701; V. MITSILEGAS, *The Limits of Mutual Trust in Europe's Area of Freedom, Security and Justice: From Automatic Inter-State Cooperation to the Slow Emergence of the Individual*, in *Yearbook of European Law*, 2012, vol. 31, n. 1, p. 319.

[91] Nella Strategia europea per i dati, ad esempio, la Commissione ha sottolineato l'importanza che gli spazi comuni europei vengano sviluppati nel "pieno rispetto delle norme in materia di protezione dei dati e conformemente alle più elevate norme disponibili in materia di cibersicurezza" (COM(2020) 66 final, p. 26). Viene altresì affermato che il "metodo europeo per la gestione dei dati", volto ad assicurare una maggiore disponibilità degli stessi da utilizzare in campo economico e per affrontare le sfide sociali, deve rispettare e promuovere i valori comuni europei (COM(2020) 66 final, p. 29).

[92] L. CHIEFFI, *Equità nella salute e nei servizi sanitari tra politiche europee e interventi statali*, in *Corti Supreme e Salute*, 2022, vol. 1, p. 189. Si vedano anche F. SALMONI, *Diritti sociali e Unione europea. Dall'ordinamento comunitario allo stato sociale europeo*, in *Scritti in onore di G. Ferrara*, Torino, 2005, p. 536 ss., e F. ROSSI DAL POZZO, *op. cit*., 2020.

[93] Un esempio tra tutti è lo Spazio di libertà, sicurezza e giustizia che, benché creato per motivi di integrazione economica, è stato collegato, con Lisbona, al concetto di cittadinanza (art. 3, par. 2, TUE). Per approfondimenti dottrinali sul tema, v. D. KOSTAKOPOULOU, *The Area of Freedom, Security and Justice and the European Union's Constitutional Dialogue*, in C. BARNARD (ed.), *The Fundamentals of EU Law Revised: Assessing the Impact of the Constitutional Debate*, OUP, Oxford, 2009, pp. 156-164; N. WALKER (ed.), *Europe's Area of Freedom, Security and Justice*, OUP, Oxford, 2004; J-C. PARIS, *The Constitution for Europe: A Legal Analysis*, CUP, Cambridge, 2006; F. CLEMENTI, *Lo spazio di libertà, sicurezza e giustizia*, in F. BASSANINI, G. TIBERI, *La Costituzione europea. Un primo commento*, Il Mulino, Bologna, 2004, pp. 104-105.

[94] Art. 179, par. 1, TFUE, in cui si riconosce come la realizzazione di un SER dovrebbe consentire di rafforzare le basi scientifiche e tecnologiche dell'Unione. Per un commento alla norma, cfr. S. GARBEN, *Articles 179-190*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *The EU Treaties and the Charter of Fundamental Rights. A Commentary*, OUP, Oxford, 2019, p. 1494 ss.

principali tappe della nascita e dello sviluppo del SER (sezione 3.1), verranno messi in evidenza gli elementi che rendono lo EHDS un'evoluzione più avanzata nella promozione della ricerca e dell'innovazione all'interno dell'Unione (sezione 3.2), delineando in filigrana possibili traiettorie di sviluppo del SER.

3.1. Le prime esperienze in materia di ricerca scientifica tra collaborazione e integrazione

L'aspirazione a creare uno spazio in cui "i ricercatori, le conoscenze scientifiche e le tecnologie circolano liberamente" [95] ha radici antiche [96]. Già l'art. 55 del Trattato di Parigi identificava la "ricerca" quale elemento chiave per l'attuazione della strategia industriale europea [97]. Analogamente, il Trattato di Roma ne faceva menzione in riferimento alla politica agricola [98], mentre il Trattato istitutivo della Comunità europea dell'energia atomica annoverava la promozione della ricerca tra gli obiettivi principali di EURATOM [99]. Tuttavia, è solo con l'Atto Unico Europeo (AUE) che viene introdotta, per la prima volta,

[95] Libro verde della Commissione sulle nuove prospettive per lo spazio europeo della ricerca, COM(2007) 161 final, del 4 aprile 2007, p. 5. Tra gli atti non vincolanti adottati dalle istituzioni con riferimento allo spazio europeo della ricerca, cfr. Risoluzione del Parlamento europeo dell'8 luglio 2021 su un nuovo spazio europeo della ricerca e dell'innovazione (2021/2524(RSP)); Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un nuovo SER per la ricerca e l'innovazione, COM(2020) 628 final, del 30 settembre 2020; Relazione della Commissione al Consiglio e al Parlamento europeo sullo spazio europeo della ricerca: Progredire insieme nell'Europa della ricerca e dell'innovazione, COM(2019) 83, del 15 febbraio 2019; Relazione della Commissione al Consiglio e al Parlamento europeo sullo spazio europeo della ricerca: Tempo di attuazione e monitoraggio dei progressi, COM(2017) 35, del 26 gennaio 2017; Relazione della Commissione al Consiglio e al Parlamento europeo sui progressi sullo spazio europeo della ricerca, COM(2014) 575 final, del 15 settembre 2014; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Un partenariato rafforzato per lo spazio europeo della ricerca a favore dell'eccellenza e della crescita, COM(2012) 392 final, del 17 luglio 2012.

[96] Cfr. R. ADAM, A. TIZZANO, *Manuale di Diritto dell'Unione Europea*, Giappichelli, Torino, 2020, p. 769.

[97] L'art. 55 Trattato istitutivo della CECA affidava all'Alta Autorità il compito di "incoraggiare le ricerche tecniche ed economiche concernenti la produzione e l'espansione del consumo del carbone e dell'acciaio, nonché la sicurezza del lavoro in dette industrie".

[98] L'art. 41 Trattato istitutivo della CEE affermava che, per consentire il raggiungimento degli obiettivi della politica agricola comune, fosse possibile prevedere "un coordinamento efficace degli sforzi intrapresi nei settori della formazione professionale, della ricerca e della divulgazione dell'agronomia, che possono comportare progetti o istituzioni finanziate in comune".

[99] Art. 2 Trattato istitutivo dell'EURATOM.

una base giuridica specifica per l'azione dell'Unione nel campo della ricerca [100].

Questa evoluzione segna un passaggio cruciale, confermando il nesso tra innovazione tecnologica e competitività delle imprese europee, ma anche evidenziando una visione della crescita economica e dello sviluppo tecnologico come strumenti al servizio del benessere dei cittadini europei e del perseguimento del bene comune [101]. La ricerca, infatti, non solo rappresenta "uno dei principali motori della crescita economica, della competitività e dell'occupazione" [102], contribuendo alla piena realizzazione del mercato interno [103], ma svolge anche un ruolo centrale nell'attuazione delle politiche pubbliche, compresa la sanità pubblica [104]. In altre parole, quindi, la libera circolazione dei ricercatori e delle conoscenze scientifiche, anche tramite mezzi digitali, costituisce un motore indispensabile per lo sviluppo economico, l'innovazione e, più in generale, per la crescita sociale dell'Unione [105].

---

[100] Artt. 130f-130Q AUE. In precedenza, per realizzare progetti di ricerca, si faceva riferimento alla clausola di flessibilità (oggi art. 352 TFUE). Il fatto che l'introduzione di una base giuridica specifica sia stata prevista dall'AUE non è un dato irrilevante, in quanto evidenzia il collegamento tra la ricerca e il mercato interno. Oltre a stabilire una data precisa per il completamento del mercato interno, l'AUE ha rafforzato i meccanismi decisionali relativi allo stesso: per questioni come la tariffa doganale comune, la libera circolazione di servizi, la libera circolazione di capitali e il ravvicinamento delle legislazioni nazionali viene previsto il voto a maggioranza qualificata. Cfr. K. LENAERTS, P. VAN NUFFEL, *op. cit*., 2011, p. 195 ss. Per ulteriori riferimenti circa l'evoluzione del mercato interno nell'ordinamento europeo, cfr. J. SNELL, *The Internal Market and the Philosophies of the European Union*, in C. BARNARD, S. PEERS, *European Union Law*, OUP, Oxford, 2020, p. 341 ss.; I. GOVAERE, *Internal Market Dynamics: On Moving Targets, Shifting Contextual Factors and the Untapped Potential of Article 3(3) TEU*, in S. GARBEN, I. GOVAERE (eds.), *op. cit*., 2020, p. 81 ss.; L. GORMLEY, *The Internal Market: History and Evolution*, in N.N. SHUIBHNE (ed.), *Regulating the Internal Market*, Edward Elgar, Cheltenham, 2006, p. 14 ss.

[101] Art. 3, par. 3, n. 1, TUE: "L'Unione instaura un mercato interno. Si adopera per lo sviluppo sostenibile dell'Europa, basato su una crescita economica equilibrata e sulla stabilità dei prezzi, su un'economia sociale di mercato fortemente competitiva, che mira alla piena occupazione e al progresso sociale, e su un elevato livello di tutela e di miglioramento della qualità dell'ambiente. Essa promuove il progresso scientifico e tecnologico".

[102] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni, Verso uno spazio europeo della ricerca, COM(2000) 6 final, del 18 gennaio 2000, p. 5. Più recentemente, v. COM(2020) 628 final, in cui si afferma che la R&I è "il motore della crescita della produttività a lungo termine"(p. 3) e Comunicazione della Commissione, Europa 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 final, del 3 marzo 2010.

[103] Ai sensi dell'art. 179, par. 2, TFUE, l'Unione si impegna a "permettere ai ricercatori di cooperare liberamente oltre le frontiere e alle imprese di sfruttare appieno le potenzialità del mercato interno".

[104] L'art. 179, par. 1, TFUE stabilisce un ulteriore obiettivo specifico dell'Unione, ossia "promuovere le azioni di ricerca ritenute necessarie ai sensi di altri capi dei trattati".

[105] Conclusioni della Presidenza del Consiglio europeo 7652/1/08, 13 e 14 marzo 2008. Dello stesso tenore sono le affermazioni compiute dalla Commissione nella Comunicazione,

È in questo contesto che, nel 2000, l'idea di creare un SER è stata formalizzata dalla Commissione europea nella Comunicazione "Verso uno spazio europeo della ricerca" [106], in cui si sottolineava la necessità di sviluppare politiche europee a favore della ricerca al fine di individuare obiettivi comuni e coordinare le diverse iniziative avviate a livello comunitario e nazionale. Nello stesso anno, il vertice europeo di Lisbona ha stabilito come obiettivo per i successivi dieci anni che l'Europa dovesse diventare un'economia basata "sulla conoscenza più competitiva e dinamica del mondo, in grado di realizzare una crescita economica sostenibile con nuovi e migliori posti di lavoro e una maggiore coesione sociale" [107]. La "Strategia Lisbona", delineata in quell'occasione, è stata poi rafforzata nel 2002 durante il vertice di Barcellona, dove si è enfatizzata l'importanza di maggiori investimenti da parte degli Stati membri per la ricerca e lo sviluppo, fissando l'obiettivo di destinare almeno il 3% del PIL a questi settori [108].

Negli anni successivi, gli obiettivi definiti con la Strategia Lisbona sono stati rimodulati nell'ambito del c.d. "Processo di Lubiana", avviato con la pubblicazione nel 2007 del Libro verde della Commissione [109] e finalizzato a rafforzare l'impegno per la costruzione del SER, individuando un quadro di obiettivi comuni ("Visione sul SER 2020") [110], tra cui quello di fare in modo che tutti gli attori possano beneficiare della c.d. "quinta libertà" (libera circolazione dei ricercatori, delle conoscenze e delle tecnologie). Cionondimeno, anche dopo che la realizzazione del SER è diventata un obiettivo esplicito dell'Unione con il Trattato di Lisbona [111], i risultati finora raggiunti non sembrano essere all'altezza delle aspettative iniziali, che avevano portato alcuni a concepire tale spazio "*as a primary pillar for the Lisbon objectives and as an engine for driving the competitiveness of Europe*" [112].

Un mercato unico per l'Europa del 21esimo secolo, in cui si sottolinea come l'affermarsi di una "quinta libertà" del mercato interno "incoraggia il diffondersi di nuove tecnologie in tutta l'UE, si presta alla creazione di reti, virtuali e reali, promuove lo sviluppo di un sofisticato settore logistico che consente la gestione integrata dei flussi di merci, energia, informazione, servizi e persone, e facilita lo scambio di conoscenze, grazie alla mobilità di lavoratori, ricercatori e studenti" (COM(2007) 724 final, del 20 novembre 2007, p. 9).

[106] COM(2000) 6 final.

[107] https://www.europarl.europa.eu/summits/lis1_it.htm.

[108] https://www.europarl.europa.eu/bulletins/pdf/01s2002_en.pdf.

[109] COM(2007) 161 final.

[110] Conclusioni del Consiglio sull'avvio del "Processo Lubiana", Verso la piena realizzazione del SER, del 30 maggio 2008 e Conclusioni del Consiglio sulla definizione di una visione per lo spazio europeo della ricerca 2020, del 2 dicembre 2008.

[111] Art. 179 TFUE.

[112] https://web.archive.org/web/20100705164904/http://ec.europa.eu/research/era/partnership/process/ljubljana_process_en.htm.

In particolare, il potenziale del SER è stato notevolmente compromesso dalla frammentazione e dalla compartimentazione degli sforzi e dei sistemi nazionali di ricerca, oltre che dalla disparità nei sistemi regolatori e amministrativi [113], derivanti dall'ampio margine di discrezionalità lasciato agli Stati membri nel definire le proprie politiche di ricerca [114]. Com'è noto, i settori della ricerca e dello sviluppo tecnologico, pur rientrando tra le competenze concorrenti dell'Unione e degli Stati membri, non sono soggetti all'applicazione del principio della *preemption*, ai sensi dell'art. 4, par. 3, TFUE [115]. Di conseguenza, l'esercizio di tale competenza da parte dell'Unione non impedisce agli Stati membri di esercitarla a loro volta.

Per via del quadro costituzionale vigente per la ricerca, le principali iniziative volte alla creazione del SER si concentrano sull'attuazione di azioni finalizzate a promuovere e rafforzare la cooperazione transfrontaliera nel campo della ricerca e il coordinamento a livello europeo delle azioni e delle politiche. Un esempio è rappresentato dallo strumento della programmazione congiunta, che consiste in una procedura per definire programmi di ricerca pubblici in settori di ricerca pan-europea/mondiale (ad es. l'ambiente, l'energia e la salute), ai quali gli Stati membri possono aderire su base volontaria [116]. Ultimamente sono state lanciate dieci tematiche di programmazione congiunta, tra cui una sulla lotta alle malattie neurodegenerative [117], un'altra sugli stili di alimentazione sana [118] e un'altra ancora sulla resistenza agli agenti antimicrobici [119].

---

[113] COM(2020) 628 final, pp. 1-2.

[114] Ai sensi dell'art. 180, par. 1, TFUE, l'azione dell'Unione nel raggiungimento degli obiettivi di ricerca e sviluppo tecnologico deve limitarsi a integrare quella degli Stati membri. In aggiunta, secondo la Dichiarazione n. 34 relativa all'art. 179 TFUE, un'eventuale azione sovranazionale deve tenere "debito conto degli orientamenti e delle scelte fondamentali delle politiche in materia di ricerca degli Stati membri".

[115] R. SCHÜTZE, *op. cit.*, 2021, p. 242-243; A. ARENA, *The Twin Doctrines of Primacy and Pre-emption*, in R. SCHÜTZE, T. TRIDIMAS (eds.), *Oxford Principles of European Union Law, Vol. I: The European Union Legal Order*, OUP, Oxford, 2018, p. 300; R. SCHÜTZE, *Supremacy Without Pre-emption? The Very Slowly Emergent Doctrine of Community Pre-emption*, in *CMLRev.*, 2006, vol. 43, n. 4, p. 1023; S. DOUGLAS-SCOTT, *Constitutional Law of the European Union*, Pearson Education Limited, London, 2002, pp. 168-169; A. ARENA, *Exercise of EU Competence and Pre-emption of Member States' Power in the Internal and External Sphere: Towards "Grand Unification"?*, in *Yearb. Eur. L.*, 2016, p. 28; A. ARENA, *Il principio della preemption in diritto dell'Unione europea. Esercizio delle competenze e ricognizione delle divergenze tra diritto derivato e diritto nazionale*, Editoriale Scientifica, Napoli, 2013.

[116] Cfr. Comunicazione della Commissione, Verso una programmazione congiunta della ricerca: cooperare per affrontare più efficacemente le sfide comuni, COM(2008) 468, del 15 luglio 2008.

[117] https://neurodegenerationresearch.eu/.

[118] https://www.healthydietforhealthylife.eu/.

[119] https://www.jpiamr.eu/.

Un'ulteriore iniziativa di supporto alla ricerca che non richiede l'adozione di specifiche azioni a livello nazionale riguarda la realizzazione di infrastrutture di ricerca. A questo proposito, nel 2002 è stato istituito un forum europeo (*European Strategy Forum for Research Infrastructure* – ESFRI), incaricato di definire una strategia coerente per lo sviluppo delle infrastrutture di ricerca in Europa [120]. Le tabelle di marcia strategiche elaborate nell'ambito di questo forum informale non impongono agli Stati membri l'attuazione di proposte specifiche o di prendere decisioni riguardanti il finanziamento e la localizzazione delle infrastrutture future. Connessa a questa iniziativa, vi è quella relativa allo *European Open Science Cloud* (EOSC), istituito per agevolare l'accesso a informazioni scientifiche aperte, gratuite e riutilizzabili. Tale iniziativa è destinata a evolversi in uno spazio di dati e una piattaforma di servizi per i dati sulla ricerca e sull'innovazione, interoperabile con gli altri spazi di dati settoriali, tra cui lo EHDS [121].

Rispetto alle iniziative menzionate finora, il ruolo dell'Unione europea nel promuovere la creazione del SER assume una rilevanza maggiore se si considerano i finanziamenti destinati a questo scopo. Dopo il raggruppamento della maggior parte degli investimenti previsti nei programmi quadro all'interno di Orizzonte 2020, quest'ultimo programma è stato sostituito da Orizzonte Europa, varato per il 2021-2027 [122]. Tramite il programma Orizzonte Europa [123], l'Unione sostiene i partenariati europei per affrontare sfide globali tramite uno sforzo congiunto tra gli Stati membri, il settore privato, le fondazioni e altri soggetti, in materia di ricerca e innovazione.

Tali collaborazioni possono prendere diverse forme, prevedendo la partecipazione della Commissione europea e di partner privati e/o pubblici (*co-programmed European partnership*) o la partecipazione finanziaria della

---

[120] https://www.esfri.eu/.

[121] Documento di lavoro dei servizi della Commissione sugli spazi comuni europei di dati, SWD(2024) 21 final, del 24 gennaio 2024, p. 45. L'impegno verso l'ampliamento e il rafforzamento dell'ecosistema europeo delle infrastrutture, in particolare attraverso un incremento degli investimenti, è stato recentemente ribadito nella Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al comitato delle Regioni, Strategia europea per le infrastrutture di ricerca e tecnologia, COM(2025) 497 final, del 15 settembre 2025, coerentemente con gli obiettivi fissati nelle proposte relative a Orizzonte Europea nel quadro finanziario pluriennale dell'UE (2028-2034) e al Fondo per la competitività.

[122] Ulteriori opportunità di finanziamento della ricerca sono offerte dai Fondi strutturali di investimento europeo, Erasmus+ e dal meccanismo per collegare l'Europa.

[123] Regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio del 28 aprile 2021 che istituisce il programma quadro di ricerca e innovazione Orizzonte Europa e ne stabilisce le norme di partecipazione e diffusione, e che abroga i regolamenti (UE) n. 1290/2013 e (UE) n. 1291/2013.

Commissione europea e di enti finanziatori pubblici nazionali (*co-funded European partnerships*) oppure di partner privati (*institutionalised European partnership*). Nel settore sanitario, le *partnership* europee avviate negli ultimi anni sono volte all'individuazione di soluzioni per migliorare la diagnosi e il trattamento di malattie rare, affrontare la resistenza antimicrobica e rafforzare la preparazione alle pandemie [124].

Il sostegno finanziario dell'Unione per la creazione del SER, benché significativo, non sembra essere sufficiente da solo a superare le inevitabili differenze che derivano dall'attuazione di politiche di ricerca nazionali che, pur essendo coordinate tra loro, mantengono una certa autonomia. L'elaborazione di ambiziose riforme per la costruzione di un SER più adatto alle sfide future è ostacolata dal fatto che gli strumenti a disposizione dell'Unione per agire in questo ambito non permettono un intervento sovranazionale particolarmente incisivo [125].

Ciò appare problematico specialmente se si considera che, a più di vent'anni dal lancio del SER, l'Unione si trova a dover affrontare un contesto storico profondamente mutato. In questo scenario, è più importante che mai creare un ambiente in cui siano i dati, ancor prima dei ricercatori, a poter circolare liberamente tra i paesi dell'Unione [126]. Attualmente, infatti, il modo di fare ricerca

---

[124] Commissione europea, Direzione generale della Ricerca e dell'innovazione, *European partnerships for health resilience*, Ufficio delle pubblicazioni dell'Unione europea, 2022.

[125] A questo proposito, si vedano, in particolare, i rilievi di Commissione e Consiglio rispettivamente nella Comunicazione, Un nuovo SER per la ricerca e l'innovazione, COM(2020) 628 final, del 30 settembre 2020, e nelle Conclusioni su un nuovo spazio europeo della ricerca, del 1° dicembre 2020. Nondimeno, nella comunicazione sulla competitività del 2025 è stata annunciata la futura presentazione di un atto legislativo sullo spazio europeo della ricerca che dovrebbe portare a un maggiore allineamento tra le priorità di finanziamento dell'Unione e degli Stati membri a sostegno della ricerca e favorire la circolazione delle conoscenze e dei talenti in tutta Europa (Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Bussola per la competitività dell'UE, COM(2025) 30 final, del 29 gennaio 2025, pp. 6-7).

[126] COM(2020) 628 final, p. 4; Conclusioni del Consiglio su un nuovo spazio europeo della ricerca, p. 14. È interessante notare come già in COM(2012) 392 final, p. 3, si affermava che "per costruire un SER competitivo a livello globale in cui l'Europa possa svolgere un ruolo di primo piano nell'affrontare le grandi sfide e in cui tutti gli Stati membri partecipano, i sistemi nazionali devono essere più aperti gli uni nei confronti degli altri e rispetto al mondo, più interconnessi e più interoperabili". Si rinvia anche alle Conclusioni del Consiglio (17649/12), in cui si legge che "l'eccellenza della ricerca dipende in particolare da strutture e infrastrutture di ricerca di livello mondiale, comprese le strutture dei partner regionali, le infrastrutture elettroniche che consentono la ricerca collaborativa ad alta intensità di computer e di dati e l'accesso remoto alle risorse e alle attrezzature, e che le infrastrutture di ricerca attirano talenti e stimolano la scienza, la ricerca, l'istruzione, l'innovazione e le opportunità commerciali" (punto 13). Viene altresì sottolineato che "l'accesso transnazionale alle infrastrutture di ricerca rimane una priorità per la comunità di ricerca in tutta Europa" (punto 14). Da qui l'esigenza

e di condividere il sapere si basa in misura sempre più rilevante sull'uso dei *Big Data* [127], il cui potenziale per migliorare la salute, la qualità della vita dei cittadini dell'Unione e le prestazioni dei sistemi sanitari è strettamente legato alla possibilità di essere condivisi [128].

3.2. Il valore aggiunto dello spazio europeo dei dati sanitari

Di fronte a simili trasformazioni, le iniziative presenti nel SER per favorire la libera circolazione dei dati appaiono insufficienti. Un'attenzione maggiore dovrebbe essere riservata alla regolamentazione dell'accesso e della condivisione dei dati, ponendo particolare attenzione alla garanzia di requisiti fondamentali quali l'interoperabilità e l'elevata qualità dei dati stessi – condizioni indispensabili per il successo di progetti di ricerca, soprattutto se di natura multicentrica. In ambito sanitario, lo EHDS compie un passo significativo in questa direzione, introducendo un quadro normativo particolarmente favorevole allo svolgimento di attività di ricerca nell'Unione.

Lo EHDS include tra le finalità legittime dell'uso secondario dei dati

---

di stabilire un quadro normativo armonizzato e di un sostegno costante dell'Unione alle attività di accesso transnazionale.

[127] COM(2015) 192 final, p. 15 e, più di recente, il documento di lavoro dei servizi della Commissione che accompagna la Comunicazione della Commissione europea, Un nuovo SER per la ricerca e l'innovazione, SWD(2020) 214 final, del 30 luglio 2020, p. 13. In dottrina, v. J. KAYE, M. PRICTOR, *Consent*, in G. LAURIE et al. (eds.), *Health Research Regulation*, CUP, Cambridge, 2021, p. 105: "*Health research is no longer a case simply of the physical measurement and intimate observation of patients. Rather, it increasingly depends upon the generation and use of data, and new analysis tools such as Artificial Intelligence (AI). Health research has been transformed by innovations in digital technologies enabling the collection, curation and management of large quantities of diverse data from multiple sources*". Si veda anche E. HAFEN, *Personal Data Cooperatives. A New Data Governance Framework for Data Donations and Precision Health*, in J. KRUTZINNA, L. FLORIDI (eds.), *The Ethics of Medical Data Donation*, Springer, Cham, 2019, pp. 141-150; S. LEONELLI, *La ricerca scientifica nell'era dei big data. Cinque modi in cui i Big Data danneggiano la scienza, e come salvarla*, Meltemi, Milano, 2018; P. GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, Editoriale scientifica, Napoli, 2021.

[128] E. TOPOL, *High-Performance Medicine: The Convergence of Human and Artificial Intelligence*, in *Nat. Med.*, 2019, vol. 25, p. 44; A. ESTEVA et al., *A Guide to Deep Learning in Healthcare*, in *Nat. Med*., 2019, vol. 25, pp. 24-29; T. DAVENPORT, R. KALAKOTA, *The Potential for Artificial Intelligence in Healthcare*, in *Future Healthc. J*., 2019, vol. 6, n. 2, pp. 94-98; D. SCHÖNBERGER, *Artificial Intelligence in Healthcare: A Critical Analysis of the Legal and Ethical Implications*, in *Int. J. Law Inf. Technol*., 2019, vol. 27, n. 2, pp. 171-203; S. ROWLAND et al., *What is the Clinical Value of mHealth for Patients?*, in *Npj Digital Medicine*, 2020, p. 1; N. FAHY et al., *Use of Digital Health Tools in Europe Before, During and After COVID-19*, European Observatory on Health Systems and Policies, Copenhagen, 2021.

sanitari elettronici anche la ricerca scientifica, intesa in senso ampio. Rientrano in tale definizione non solo i progetti finalizzati allo sviluppo e all'innovazione di prodotti o servizi, ma anche le attività di addestramento, prova e valutazione di algoritmi [129], a condizione che contribuiscano alla sanità pubblica, alla valutazione delle tecnologie sanitarie, alla sicurezza sociale o al miglioramento della qualità e della sicurezza delle cure, dei medicinali o dei dispositivi medici [130]. Di conseguenza, i soggetti impegnati in queste attività potranno beneficiare del meccanismo di accesso ai dati per finalità secondarie previsto dallo EHDS, presentando apposita domanda agli organismi competenti [131]. Per conoscere quali dati sono disponibili e valutarne la qualità e l'utilità, sarà sufficiente consultare i cataloghi nazionali delle serie di dati, pubblicati sui siti web degli organismi preposti [132] e resi interoperabili con i cataloghi europei e con quelli gestiti da infrastrutture di ricerca o piattaforme di condivisione dati [133].

Tra le disposizioni particolarmente favorevoli alla comunità scientifica figura anche la possibilità, per gli organismi responsabili per l'accesso ai dati, di applicare tariffe agevolate ai ricercatori universitari che ne facciano richiesta per fini di ricerca [134]. Inoltre, gli Stati membri potranno autorizzare l'accesso ai dati anche nel caso in cui un interessato abbia esercitato il proprio diritto di *opt-out*, purché i dati siano destinati a enti pubblici incaricati di svolgere compiti connessi alla sanità pubblica e la finalità perseguita sia di evidente interesse pubblico, come, ad esempio, nel caso di studi su malattie rare o su minacce sanitarie emergenti [135].

Inoltre, la ricerca multicentrica transnazionale potrà beneficiare della futura piattaforma transfrontaliera per l'uso secondario (HealthData@EU), concepita per facilitare lo scambio di dati a livello dell'Unione attraverso l'interconnessione dei punti di contatto nazionali [136]. In questo contesto, le infrastrutture di ricerca come quelle coordinate dallo ESFRI o dallo EOSC potranno essere autorizzate a partecipare a HealthData@EU [137], usufruendo di

[129] Considerando 61 EHDS.

[130] Art. 53, par. 1, lett. e), EHDS.

[131] Artt. 68 e 69 EHDS.

[132] Art. 77 EHDS.

[133] Considerando 86 EHDS.

[134] Art. 62, par. 1, EHDS.

[135] L'art. 71 EHDS specifica anche che per accedere a tali dati occorre dimostrare la mancanza di sistemi che consentono di ottenerli con mezzi alternativi in modo tempestivo ed efficace a condizioni equivalenti, e soddisfare specifiche condizioni previste per presentare una domanda di accesso ai dati o una richiesta di dati. Cfr. anche il considerando 54 EHDS.

[136] Art. 75 e considerando 80 EHDS.

[137] Art. 75, par. 4, EHDS.

un'ampia gamma di servizi che includono il supporto nella gestione delle richieste transfrontaliere dei dati, la connettività dei dati e l'accesso a banche dati transfrontaliere.

Infine, a differenza del SER, la cui attuazione effettiva viene lasciata sostanzialmente agli Stati membri, la realizzazione di uno EHDS per i cittadini, i ricercatori e gli innovatori può contare su una strategia più strutturata. Tale strategia combina l'adozione di atti legislativi vincolanti con la creazione di nuovi ecosistemi e infrastrutture digitali, sostenuti da una pluralità di programmi di finanziamento.

A livello normativo, il quadro favorevole delineato dallo EHDS per incentivare l'utilizzo dei dati a fini di ricerca e innovazione in tutta l'Unione è ulteriormente rafforzato da alcune disposizioni orizzontali contenute nel DGA e nel DA. Si pensi, ad esempio, alla possibilità per gli Stati membri di introdurre meccanismi di altruismo dei dati, mediante i quali gli interessati o i titolari dei dati possono volontariamente metterli a disposizione per obiettivi di interesse generale, come l'assistenza sanitaria, il miglioramento dei servizi pubblici e il sostegno alla ricerca scientifica [138]. Ciò dovrebbe contribuire a creare bacini di dati ampi, gestiti tramite organizzazioni per l'altruismo dei dati, di cui potranno beneficiare una pluralità di attori, tra cui enti di ricerca e ricercatori. Come già menzionato, in ambito sanitario, il funzionamento di tali pratiche potrà essere ulteriormente dettagliato attraverso un codice di condotta elaborato dalla Commissione, che integrerà quanto previsto dal DGA [139].

Al fine di rendere i dati più facilmente accessibili per finalità di ricerca scientifica di interesse pubblico, il DGA promuove anche lo sviluppo, da parte degli enti pubblici detentori di dati protetti, di un approccio armonizzato, attraverso l'introduzione di procedure amministrative semplificate e la formattazione standardizzata dei dati [140]. Questo obiettivo riveste un'importanza cruciale per favorire l'integrazione e l'interoperabilità dei dati provenienti da fonti diverse, non solo nel settore pubblico (oggetto del DGA), ma anche nel settore privato, al centro dell'intervento del DA. Quest'ultimo, infatti, stabilisce requisiti essenziali di interoperabilità che potranno essere ulteriormente specificati mediante atti delegati della Commissione. Tali requisiti saranno vincolanti per tutti i partecipanti agli spazi comuni europei dei dati, sia nel caso in cui offrano dati o servizi ad altri partecipanti, sia quando facilitino la condivisione di dati all'interno degli stessi [141].

---

[138] Artt. 2, par. 6, e 16 DGA.

[139] Art. 22 DGA.

[140] Considerando 16 DGA.

[141] Art. 33 DA.

Passando al secondo livello di intervento, oltre ai programmi di finanziamento Orizzonte Europa e al Meccanismo per collegare l'Europa di cui beneficia anche il SER [142], lo EHDS può contare anche sul sostegno dei programmi Europa Digitale (DIGITAL) [143] e EU4Health [144]. Questi ultimi saranno fondamentali per la creazione e il funzionamento dell'ecosistema europeo dei dati sanitari, fornendo le infrastrutture e i servizi necessari per processarli.

In particolare, attraverso il programma DIGITAL, la Commissione può finanziare cinque aree prioritarie: il calcolo ad alte prestazioni, l'intelligenza artificiale, la cibersicurezza, le competenze digitali avanzate, nonché le capacità digitali e l'interoperabilità [145]. A queste si affianca il sostegno all'istituzione di un Centro di supporto per gli spazi di dati, il cui ruolo sarà determinante nel fornire assistenza al Comitato europeo per l'innovazione in materia di dati [146] e nel coordinare le iniziative sviluppate all'interno dei diversi spazi comuni. Il Centro sarà chiamato a garantire coerenza tra gli spazi, promuoverne l'interoperabilità e favorire sinergie ed economie di scala [147]. Per i primi due anni di attuazione del programma, la Commissione ha stanziato circa 410 milioni di euro destinati, *inter alia*, allo sviluppo degli spazi comuni europei dei dati e dell'infrastruttura *cloud-to-edge* [148].

Parallelamente, nell'ambito del quinto piano di lavoro del programma EU4Health, sono stati assegnati circa 40 milioni di euro a sostegno della digitalizzazione della sanità, con un incremento di oltre il 50% rispetto al 2024.

---

[142] Regolamento (UE) 2021/695 e regolamento (UE) 2021/1153 del Parlamento europeo e del Consiglio del 7 luglio 2021 che istituisce il meccanismo per collegare l'Europa e abroga i regolamenti (UE) n. 1316/2013 e (UE) n. 283/2014. Questi programmi sono finalizzati, *inter alia*, a "sviluppare, promuovere e far progredire l'eccellenza scientifica", anche nel settore sanitario (art. 3, par. 2, lett. a), regolamento (UE) 2021/695) nonché a consentire "lo sviluppo e il rafforzamento delle risorse di dati di qualità e dei corrispondenti meccanismi di scambio" (art. 5, regolamento (UE) 2021/694).

[143] Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240.

[144] Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio del 24 marzo 2021 che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 ("programma UE per la salute") (EU4Health) e che abroga il regolamento (UE) n. 282/2014. Il programma EU4Health verrà integrato anche da altri strumenti, come il dispositivo per la ripresa e la resilienza e il Fondo europeo di sviluppo regionale, che sosterranno il collegamento degli Stati membri alle infrastrutture europee all'interno dello EHDS.

[145] Art. 3 regolamento (UE) 2021/694.

[146] Art. 29 DGA.

[147] SWD(2024) 21 final, p. 11.

[148] *Ibid.* p. 8. L'interesse strategico dell'Unione a investire sullo sviluppo dei *cloud* emerge chiaramente dallo studio condotto da P. FOLEY et al., *Economic Value of Data Flows*, Publications Office of the European Union, Luxembourg, 2023, p. 184.

La maggior parte delle risorse sarà destinata al potenziamento dell'infrastruttura transfrontaliera per l'uso primario dei dati (MyHealth@EU), alla creazione di quella per l'uso secondario (HealthData@EU), nonché all'istituzione di un centro di supporto volto a promuovere l'adozione del formato europeo per lo scambio delle cartelle cliniche elettroniche [149].

L'approccio multilivello adottato dalla Commissione nell'ambito della Strategia europea per i dati lascia intravedere un futuro potenzialmente più promettente per lo EHDS rispetto al SER, la cui attuazione continua a dipendere in larga misura dalla volontà degli Stati membri di cooperare tra loro e con le istituzioni dell'Unione. Anche se in un ambito settoriale più circoscritto, lo EHDS potrebbe, nel tempo, contribuire al raggiungimento di alcuni degli obiettivi originariamente perseguiti con la creazione del SER. In particolare, se adeguatamente coordinato con l'EOSC e con le infrastrutture europee di ricerca pertinenti – quali quelle dedicate alla gestione dei dati di ricerca in ambito sanitario, alle raccolte di biobanche e ai dati di diagnostica per immagini – lo EHDS potrà offrire ai ricercatori, agli innovatori e ai decisori pubblici strumenti più efficaci e sicuri per l'accesso, la condivisione e il riutilizzo dei dati all'interno dell'Unione.

4. Lo spazio europeo dei dati sanitari come strumento di attuazione della Carta dei diritti fondamentali

Le riflessioni svolte fin qui sul contributo dello EHDS alla promozione della ricerca e dell'innovazione in Europa hanno permesso di spostare il focus della nostra analisi dagli obiettivi dello EHDS di natura più marcatamente economica a quelli di carattere sociale, sebbene – occorre ribadirlo – una netta distinzione tra gli stessi non sia possibile. Come emerso, la ricerca scientifica funge infatti non solo da motore per la crescita economica, ma anche da catalizzatore per il progresso sociale, soprattutto quando è orientata alla realizzazione di interessi pubblici. Questa duplice natura caratterizza anche i dati e, così, tutte le attività che si fondano sul loro utilizzo. A questo proposito, si può osservare che, sebbene il legislatore europeo abbia mantenuto un approccio prudente nell'applicare logiche di mercato in settori connessi all'uso dei dati, specialmente quando si tratta di dati personali, con il perfezionarsi delle tecniche di raccolta, elaborazione e analisi dei dati, è cresciuta la consapevolezza

[149] Allegato I decisione di esecuzione della Commissione relativa al finanziamento del programma d'azione dell'Unione in materia di salute ("programma EU4Health") e all'adozione del programma di lavoro per il 2025, pp. 9 e 135-140.

delle potenzialità derivanti dallo sfruttamento del valore dei dati in termini di sviluppo economico e di miglioramento del benessere collettivo [150].

Da qui deriva, come anticipato all'inizio della sezione precedente, la scelta di parlare di uno "spazio" europeo dei dati sanitari in cui le logiche del mercato vengono piegate alle esigenze e ai bisogni dei singoli e della collettività. Per massimizzare l'utilità economica e sociale dei dati sanitari [151], l'uso e la condivisione di questi sono promossi con finalità che vanno dall'ottimizzazione dell'assistenza e della programmazione sanitaria (uso primario), al sostegno alla ricerca scientifica e all'innovazione (uso secondario), nel rispetto dei valori e dei diritti propri del costituzionalismo europeo, che pone al centro l'individuo e le sue libertà fondamentali. In questa prospettiva lo EHDS può essere inteso come strumento di attuazione dei diritti della Carta e, in particolare modo, del diritto alla salute (sezione 4.1) e alla protezione dei dati personali (sezione 4.2).

4.1. Il diritto fondamentale alla salute

In Europa, nonostante le differenze – specialmente riguardo alla modalità di finanziamento – tra i sistemi sanitari degli Stati membri [152], la tutela della

---

[150] Il valore economico e sociale dei dati viene riconosciuto pienamente nella Strategia europea per i dati. In questa Comunicazione, la Commissione non solo afferma che "i dati sono la linfa vitale dello sviluppo economico", ma evidenzia anche come questi, da un lato, consentono "un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici" e, dall'altro, costituiscono una risorsa "fondamentale per far fronte alla sfide sociali, climatiche e ambientali, contribuendo allo sviluppo di società più sane, più prospere e più sostenibili" (pp. 2-3). Nella stessa Comunicazione, viene evidenziato che "l'Europa mira a sfruttare i vantaggi di un migliore utilizzo dei dati, compresi una maggiore produttività e mercati competitivi, ma anche miglioramenti in materia di salute e benessere, ambiente, amministrazione trasparente e servizi pubblici" (COM(2020) 66 final, p. 1).

[151] Come osservato dall'EDPS, "*personal data enable better understanding of diseases, the development of new therapies and generally improvement of quality of life*" (EDPS, *A Preliminary Opinion on Data Protection and Scientific Research*, 2020, p. 6). Sul punto, si rinvia anche a OECD, *Health in the 21st Century. Putting Data to Work for Stronger Health Systems*, OECD Publishing, Parigi, 2019 e OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Parigi, 2015. In dottrina, S. MARJANOVIC et al., *Understanding Value in Health Data Ecosystems*, in *Rand Health Quarterly*, 2018, vol. 7, n. 2, individuano tre settori in cui l'accesso ai dati sanitari presenta le maggiori potenzialità per la ricerca, la sanità pubblica e la farmacovigilanza, l'erogazione dei servizi di assistenza sanitaria. Inoltre, con riferimento al potenziale dei dati delle sperimentazioni cliniche per individuare gli effetti collaterali dei farmaci, si veda A.S. KESSELHEIM, M.M. MELLO, *Confidentiality Laws and Secrecy in Medical Research: Improving Public Access to Data on Drug Safety*, in *Market Watch*, 2005, vol. 26, n. 2, p. 487.

[152] G. DI FEDERICO, S. NEGRI, *Unione europea e salute. Principi, azioni, diritti e standard qualitativi*, Cedam, Padova, 2019, p. 65 ss.

salute rappresenta un diritto fondamentale, che trova il suo addentellato costituzionale nell'art. 35 della Carta [153], oltre che – all'evenienza – nelle carte nazionali dei singoli Stati membri. Così come è stato ben espresso dall'Avvocato Generale Ruiz-Jarabo Colomer in *Stamatelaki*, la salute non è da intendersi solo "sotto l'angolatura di costi sociali e difficoltà economiche latenti", ma piuttosto come "un diritto soggettivo, indipendente dal rapporto del singolo con la previdenza sociale" [154]. È in questa prospettiva che il diritto alla salute, nella sua versione digitale, trova ulteriore riconoscimento nella Dichiarazione sui principi e i diritti digitali, adottata con l'obiettivo di specificare "come si dovrebbero applicare nell'ambiente digitale" i valori e i diritti fondamentali dell'Unione propri del mondo *offline* [155].

La Dichiarazione stabilisce che ogni individuo ha diritto ad accedere ai servizi sanitari digitali attraverso un'identità digitale sicura e universalmente riconosciuta. A tal fine, le istituzioni europee si impegnano a garantire in tutta l'Unione "un accesso fluido, sicuro e interoperabile a servizi pubblici digitali concepiti per soddisfare le esigenze delle persone in modo efficiente, compresi in particolare i servizi sanitari e assistenziali digitali, segnatamente l'accesso alle cartelle cliniche elettroniche" [156]. L'assunzione di un impegno simile si allinea agli sforzi compiuti dall'Unione per la digitalizzazione del settore sanitario, che dovrebbe tradursi in un aumento del livello di qualità delle

---

[153] Sulla portata e sulla natura dell'art. 35 della Carta, si rinvia a G. DI FEDERICO, *Art. 35*, in R. MASTROIANNI et al. (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017, p. 670 ss.; A. DE RUIJTER, *EU Health Law & Policy: The Expansion of EU Power in Public Health and Health Care*, OUP, Oxford, 2019, p. 39 ss. Per un approfondimento sui fondamenti costituzionali del diritto alla salute nell'ordinamento europeo, cfr. G. DI FEDERICO, *Access to Healthcare in the Post-Lisbon Era and the Genuine Enjoyment of EU Citizens' Rights*, in L.S. ROSSI, F. CASOLARI (eds.), *The EU after Lisbon. Amending or Coping with Existing Treaties?*, Springer, Cham, 2014, p. 181.

[154] Conclusioni dell'Avvocato generale Ruiz-Jarabo Colomer, presentate l'11 gennaio 2007, causa C-444/05, *Stamatelaki*, ECLI:EU:C:2007:24, punto 40.

[155] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01), punto 3. La Dichiarazione propone un modello di trasformazione digitale che pone al centro le persone (antropocentrico) e assicura il rispetto dei "diritti fondamentali, lo Stato di diritto, la democrazia, l'inclusione, l'accessibilità, l'uguaglianza, la sostenibilità, la resilienza, la sicurezza, il miglioramento della qualità della vita, la disponibilità di servizi e il rispetto dei diritti e delle aspirazioni di ognuno" (considerando 6). Sul punto, in dottrina, v. A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE*, 2023, n. 15, pp. 322-323; P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *DUE*, 2022, pp. 163-172; E. QUINN, *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *Verfassungsblog.de*, 2022; L. CIANCI, *Dichiarazione europea sui diritti e principi digitali: quid pluris?*, in *DPCE*, 2022, p. 381 ss.

[156] Punto 7, lett. c), Dichiarazione comune sui principi e diritti digitali.

cure nell'Unione, contribuendo altresì a garantire un accesso paritario all'assistenza sanitaria [157].

La digitalizzazione delle cartelle cliniche, ad esempio, può favorire una gestione più efficace delle principali patologie croniche, come il cancro e le malattie rare, assicurando al contempo parità di accesso a servizi sanitari di elevata qualità in tutta l'Unione [158]. Proprio per questi motivi, nella Comunicazione sulla Bussola per il digitale, la Commissione ha sottolineato l'importanza di garantire che il 100% delle cartelle cliniche elettroniche sia accessibile ai cittadini europei [159], attraverso l'adozione di specifiche tecniche comuni per la condivisione dei dati sanitari, la promozione dell'interoperabilità, lo sviluppo di infrastrutture sicure e l'attuazione di misure volte a incentivare la fiducia dei cittadini nella condivisione dei propri dati sanitari con i professionisti del settore [160].

In questo scenario, lo EHDS rappresenta lo sviluppo normativo più recente volto a dare attuazione al diritto soggettivo "di accesso a un'assistenza sanitaria moderna e globale" [161]. Questo si realizza sia in modo diretto, attraverso le norme relative all'uso primario, sia in modo indiretto, tramite quelle concernenti l'uso secondario dei dati sanitari. Le prime consentono alle persone fisiche di esercitare il proprio diritto alla salute, riconoscendo loro la possibilità di accedere ai dati sanitari contenuti nelle proprie cartelle cliniche e di richiederne la portabilità a livello nazionale e transfrontaliero [162]. Per garantire l'effettivo esercizio di questi diritti, lo EHDS richiede agli Stati membri di

---

[157] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana, COM(2018) 233 final, del 25 aprile 2018, p. 5.

[158] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Plasmare il futuro digitale, COM(2020) 67 final, del 19 febbraio 2020, p. 12.

[159] Già nella revisione intermedia dell'applicazione della strategia sul mercato unico digitale, la Commissione aveva insistito sull'importanza di garantire ai cittadini l'accesso alle proprie cartelle elettroniche, oltre che di favorire lo sviluppo di infrastrutture per i dati al fine di promuovere la ricerca, la prevenzione delle malattie e la medicina personalizzata. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, COM(2017) 228 final, del 10 maggio 2017, p. 19.

[160] Comunicazione della Commissione al Parlamento europeo e al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Bussola per il digitale 2030: il modello europeo per il decennio digitale, COM(2021) 118 final, del 9 marzo 2021, pp. 12-13.

[161] Risoluzione del Parlamento europeo del 10 luglio 2020 sulla strategia dell'UE in materia di sanità pubblica dopo la crisi della COVID-19 (2020/2691(RSP)), punto F.

[162] Artt. 3, 5-10 EHDS.

istituire servizi di accesso ai dati sanitari elettronici e servizi di delega [163]. Inoltre, sempre in quest'ottica, sono imposti precisi obblighi ai professionisti sanitari [164], è resa obbligatoria la partecipazione all'infrastruttura MyHealth@EU [165] e vengono fissati requisiti essenziali di sicurezza e interoperabilità per i sistemi di cartelle cliniche elettroniche, nonché per i prodotti interoperabili con tali sistemi [166].

D'altra parte, le norme relative all'uso secondario consentono di realizzare il diritto soggettivo alla salute in modo indiretto, permettendo agli individui di beneficare del valore generato dallo sfruttamento dei dati sanitari. Le garanzie previste dallo EHDS per assicurare il rispetto del diritto fondamentale alla protezione dei dati personali, insieme alla definizione di regole comuni quanto all'uso degli stessi [167] e all'istituzione di un'infrastruttura tecnica dedicata (HealthData@EU) [168], sono pensate per garantire un accesso tempestivo e transfrontaliero ai dati sanitari. Ciò consentirà di prevenire, rilevare e rispondere rapidamente alle emergenze sanitarie; migliorare la comprensione, la prevenzione, l'individuazione precoce, la diagnosi e la cura di malattie come il cancro; sviluppare medicinali, vaccini innovativi e dispositivi medici.

Infine, l'aumento di disponibilità di dati sanitari nell'Unione contribuirà in modo significativo alla creazione di un'Unione europea della Salute (UES) [169], di cui lo EHDS rappresenta un tassello cruciale [170]. In particolare, la messa a disposizione di dati di qualità da parte di attori pubblici e privati all'interno di ambienti sicuri di trattamento dovrebbe permettere di sostenere il lavoro del servizio interno alla Commissione HERA (*Health Emergency Response Authority*) [171], dell'EMA e dell'ECDC [172], nonché di supportare la realizzazione

[163] Art. 4 EHDS.

[164] Art. 11 EHDS.

[165] Art. 23 EHDS.

[166] Artt. 30-49 e allegato II EHDS.

[167] Art. 51 ss. EHDS.

[168] Art. 75 EHDS.

[169] Comunicazione della Commissione, Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero, COM(2020) 724 final, dell'11 novembre 2020.

[170] Considerando 1 EHDS e proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, COM(2022) 197 final, del 3 maggio 2020, pp. 4-5. Si veda anche la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, L'Unione europea della salute: agire insieme per la salute delle persone, COM(2024) 206 final, del 22 maggio 2024.

[171] Decisione della Commissione del 16 settembre 2021 che istituisce l'Autorità per la preparazione e la risposta alle emergenze sanitarie, C/2021/6712, final.

[172] Nell'ambito delle iniziative relative all'UES è stato ampliato il mandato di EMA e

della strategia farmaceutica per l'Europa [173] e della missione dell'Unione dedicata al cancro [174] nel piano sulla lotta contro il cancro [175].

Nell'assicurare la tutela del diritto alla salute attraverso la promozione dell'uso e della condivisione di dati sanitari elettronici, compresi quelli personali, le norme dello EHDS danno attuazione anche al diritto sancito dall'art. 8 della Carta [176]. Più nello specifico, come verrà illustrato nelle pagine successive, all'interno del quadro delineato dallo EHDS si realizza una particolare concezione del diritto alla protezione dei dati personali non tanto come diritto connesso alla riservatezza (art. 7 della Carta), quanto piuttosto come diritto al trattamento dei dati personali secondo regole e principi codificati.

4.2. Il diritto fondamentale alla protezione dei dati personali

Prima di affermarsi come diritto autonomo [177], il diritto alla protezione dei dati personali ha origine come derivazione del diritto alla riservatezza [178],

---

ECDC tramite l'adozione, rispettivamente, del regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici; regolamento (UE) 2022/2370 del Parlamento europeo e del Consiglio del 23 novembre 2022 recante modifica del regolamento 851/2004, con il quale si crea un Centro europeo per la prevenzione e il controllo delle malattie.

[173] https://health.ec.europa.eu/medicinal-products/pharmaceutical-strategy-europe_it. Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia farmaceutica per l'Europa, COM(2020) 761 final, del 25 novembre 2020, con cui la Commissione ha espresso l'intenzione di riesaminare la normativa farmaceutica per migliorare la sicurezza dell'approvvigionamento e affrontare le carenze di medicinali in situazioni di emergenza.

[174] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/eu-mission-cancer_en.

[175] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union/cancer-plan-europe_it.

[176] Art. 8 della Carta. Per un commento, cfr. H. KRANENBORG, *Article 8 – Protection of Personal Data*, in S. PEERS et al. (eds.), *The EU Charter of Fundamental Rights. A Commentary*, Hart Publishing, Oxford, 2022, p. 223 ss.; T. LOCK, *Articles 6-19*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019, p. 2121; F. POCAR, M.C. BARUFFI, A. ADINOLFI, *Commentario breve ai Trattati dell'Unione europea*, Cedam, Assago, 2014, p. 1682 ss.

[177] O. LINSKEY, *The Foundations of EU Data Protection Law*, OUP, Oxford, 2015, p. 130. Per una ricostruzione dei passaggi che hanno portato all'introduzione dell'art. 8 della Carta nell'ordinamento europeo, cfr. P. VOGIATZOGLOU, P. VALCKE, *Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law*, in E. KOSTA, R. LEENES, I. KAMARA, *Research Handbook on Privacy and Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, pp. 11-49.

[178] Art. 7 della Carta. Sulla distinzione tra gli artt. 7 e 8 della Carta, le Spiegazioni a questa

tradizionalmente definito in termini negativi quale "diritto a essere lasciato solo" [179]. Tuttavia, rispetto a quest'ultimo, il diritto alla protezione dei dati personali si consolida come diritto (di contenuto positivo) al controllo sul flusso di informazioni che assicura all'individuo il diritto all'autonomia e all'autodeterminazione [180], legandosi strettamente al diritto alla dignità umana [181].

---

non forniscono indicazioni, in quanto affermano solamente che il diritto alla protezione dei dati personali si fonda sull'art. 286 EC, la direttiva 1995/46/CE (DPD) e l'art. 8 della Convenzione europea per i diritti dell'uomo e della Convenzione 108+, riconoscendo la possibilità di prevedere dei limiti a tale diritto sulla base della DPD e dell'art. 52 della Carta. Per alcuni riferimenti dottrinali sulla relazione tra il diritto alla privacy e il diritto alla protezione dei dati personali, si rinvia a O. LINSKEY, *op. cit*., 2015, p. 89 ss.; R. GELLERT, S. GUTWIRTH, *The Legal Construction of Privacy and Data Protection*, in *CLSR*, 2013, vol. 29, pp. 522-530; O. LINSKEY, *Deconstructing Data Protection: The "Added-value" of a Right to Data Protection in the EU Legal Order*, in *Int. Comp. Law Q*, 2014, vol. 63, p. 569 ss.; G. ZANFRIN-FORTUNA, *Article 16 TFEU – Commentary*, in H-J. BLANKE, S. MANGIAMELI (eds.), *The Treaty on the Functioning of the European Union. A Commentary*, Springer, Berlin, 2021, p. 427; D.J. SOLOVE, *The Digital Person: Technology, and Privacy in the Information Age*, NYU Press, New York, 2004, p. 20; Y. POULLET, *Data Protection Legislation: What is at Stake for our Society and for Democracy?*, in *Comput. Law Secur. Rev.*, 2009, vol. 25, p. 211; J. KOKOTT, C. SOBOTTA, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *Int. Data Priv. Law*, 2013, vol. 3, p. 222; J.A. CANNATACI, J.P. MIFSUD-BONNICI, *Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty*, in *ICT*, 2015, vol. 14, p. 8; C. DE TERWANGNE, *Privacy and Data Protection in Europe: Council of Europe Convention 108 and the European Union's GDPR*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit.*, 2022, p. 12.

[179] S. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harv. L. Rev.*, 1890, vol. 5, p. 4 ss. Si veda, altresì, K. HUGHES, *The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse*, in B. ROESSLER, D. MOKROSINSKA (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, CUP, Cambridge, 2015, pp. 225-243; D.J. SOLOVE, P.M. SCHWARTZ, *Information Privacy Law*, Wolters Kluwer, Alphen aan den Rijn, 2020, p. 10.

[180] In dottrina, cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 1995, p. 122; G. FINOCCHIARO, *Introduzione al Regolamento europeo alla protezione dei dati*, in *Nuove leggi civ. comm*., 2017, p. 2; A. ROUVROY, Y. POULLET, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in S. GUTWIRTH et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 45-76.

[181] Art. 1 della Carta. Cfr. L. CALIFANO et al., *La protezione dei dati personali, natura, garanzie e bilanciamento di un diritto fondamentale*, Giappichelli, Torino, 2023, p. 23 ss. e parere dell'EDPS n. 04/2015, Verso una nuova etica digitale. Dati, dignità e tecnologia, p. 4. Sul controverso rapporto tra il diritto alla dignità e il diritto alla protezione dei dati personali, si rinvia a O. LYNSKEY, *op. cit*., 2015, p. 100; L. FLORIDI, *On Human Dignity as a Foundation for the Right to Privacy*, in *Philosophy & Technology*, 2016, vol. 29, p. 307; G. BOGNETTI, *The Concept of Human Dignity in European and US Constitutionalism*, in G. NOLTE (ed.), *European and US Constitutionalism*, CUP, Cambridge, 2005, p. 90; R. BROWNSWORD, *Freedom of Contract, Human Rights and Human Dignity*, in D. FRIEDMAN, D. BARAK-EREZ (eds.), *Human Rights in Private Law*, Hart Publishing, London, 2001, p. 188.

La costituzionalizzazione del diritto alla protezione dei dati personali nella Carta non ha fatto venire meno la forte connessione con il diritto al rispetto della vita privata e familiare di cui all'art. 7 della Carta. Ciò in ragione anche dell'attività ermeneutica della Corte, specialmente quella riguardante la direttiva 1995/46/CE (DPD) [182], in cui l'autonomia concettuale del diritto alla protezione dei dati personali appare sfumata.

In *Promusicae*, il diritto previsto all'art. 8 della Carta viene inteso come una sottocategoria del più ampio diritto alla privacy [183]. Similmente, in *Volker*, la Corte afferma che i due diritti sono "strettamente" connessi [184], mentre l'Avvocato Generale Sharpston distingue tra il "classico" diritto alla privacy e il più "moderno" diritto alla protezione dei dati personali [185]. Da ultimo, in *Google Spain*, la Corte si spinge fino all'elaborazione di una sorta di crasi dei due diritti, riferendosi a questi come il diritto dell'interessato al "rispetto della sua vita privata con riguardo al trattamento dei dati personali" [186].

Sulla base di questa interconnessione tra il diritto alla protezione dei dati personali e il diritto alla privacy, l'art. 8 della Carta è stato concepito come "*prohibitive right*" [187]. Questo tipo di approccio implica che, di regola, ogni trattamento di dati deve considerarsi non ammesso, salvo in quelle situazioni eccezionali in cui il trattamento è effettuato in modo lecito e rispettoso dei principi di limitazione delle finalità o di minimizzazione dei dati [188]. Un caso emblematico in tal senso è *Digital Rights Ireland*, dove i giudici hanno stabilito che il regime predisposto dalla direttiva 2006/24/CE sulla conservazione

---

[182] O. LYNSKEY, *op. cit.*, 2015, p. 173.

[183] Sentenza della Corte del 29 gennaio 2008, causa C-275/06, *Promusicae*, ECLI:EU: C:2008:54, punto 64.

[184] Sentenza della Corte del 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker*, ECLI:EU:C:2010:662, punto 47.

[185] Conclusioni dell'Avvocato generale Sharpston del 17 giugno 2010, cause riunite C-92/09 e C-93/09, *Volker*, ECLI:EU:C:2010:353, punto 71.

[186] Sentenza della Corte del 13 maggio 2014, causa C-131/12, *Google Spain*, ECLI: EU: C:2014:317, punto 74. Cfr. C. AMALFITANO, *General Principles of EU Law and the Protection of Fundamental Rights*, Edward Elgar Publishing, Cheltenham, 2018, pp. 118-119, in cui *Google Spain* viene citata come "*one of the most well-known examples*" dell'approccio evolutivo nell'interpretazione delle disposizioni della Carta per proteggere un nuovo diritto alla "*digital privacy*".

[187] G. GOZALEZ FUSTER, R. GELLERT, *The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right*, in *IRLCT*, 2012, vol. 26, p. 531. Al contrario, la concettualizzazione del diritto alla protezione dei dati personali come "*permissive right*" comporta che il trattamento dei dati personali sia, in linea di principio, consentito e legittimo. Questa tesi è abbracciata soprattutto da coloro che ritengono che i diritti *ex* artt. 7 e 8 della Carta siano distinti. Per una ricostruzione del dibattito dottrinale sorto in relazione alla concettualizzazione del diritto alla protezione dei dati personali, cfr. P. VOGIATZOGLOU, P. VALCKE, *op. cit.*, 2022, p. 23 ss.

[188] Art. 8, par. 2, Carta.

dei dati a fini di prevenzione, indagine, accertamento e perseguimento di gravi reati costituisce un'ingerenza con il diritto alla protezione dei dati per il solo fatto di prevedere "un trattamento dei dati personali" [189].

Sebbene in linea con la necessità di proteggere l'autonomia informativa delle persone fisiche e garantire loro il pieno controllo sui dati personali, un'interpretazione simile del diritto alla protezione dei dati personali rischia di non soddisfare pienamente le esigenze dell'attuale contesto storico. In un'epoca caratterizzata da una crescente pressione ad assicurare l'uso e la condivisione dei dati in modo che gli stessi interessati possano beneficiare del loro valore economico e sociale, il legislatore europeo ha riconosciuto, sia nel GDPR che nello EHDS, l'importanza di un equilibrio tra il rafforzamento del controllo sui dati personali e l'utilizzo legittimo di tali dati.

Per non compromettere l'efficacia di questi due strumenti – lo vedremo nella seconda parte del presente lavoro [190] – sarebbe opportuno che l'interprete fornisse una lettura degli stessi, adottando una concettualizzazione del diritto di cui all'art. 8 della Carta non come diritto che pone, salvo specifiche condizioni, un generale divieto al trattamento, ma piuttosto come diritto ad avere "*a (set of) rule(s) regulating the processing of personal data*" [191]. Ciò significa garantire all'interessato la possibilità di opporsi a trattamenti illegittimi e, più in generale, esercitare un controllo sul trattamento e sui dati stessi [192].

Questa interpretazione del diritto alla protezione dei dati personali trova conferma, innanzitutto, nella scelta dei redattori della Carta di distinguere tra il diritto alla riservatezza (art. 7) e il diritto alla protezione dei dati personali (art. 8) [193], marcando così la differenza rispetto anche al diritto alla dignità

---

[189] Sentenza dell'8 aprile 2014, causa C-293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, punto 36. In questa occasione, la Corte ha, in primo luogo, affermato che la direttiva in questione non viola il "contenuto essenziale" del diritto alla protezione dei dati, per via della presenza di una serie di principi di protezione e sicurezza dei dati che impongono agli Stati di adottare misure tecniche e organizzative volte a mitigare il rischio di distruzione accidentale o illecita, perdita o alterazione accidentale dei dati (punto 40). In secondo luogo, tuttavia, la Corte ha riconosciuto l'incompatibilità della direttiva sulla conservazione dei dati con l'art. 8 della Carta, dal momento che le misure in essa contenute sono state considerate non proporzionate all'obiettivo di prevenzione di reati gravi che attentano alla sicurezza nazionale (punti 45 ss.). Cfr. G. ZANFIR-FORTUNA, *Follow the (Personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package*, in *EDPS at 20 Anniversary Volume* (in corso di pubblicazione), pp. 7-8.

[190] In particolare, cfr. capitolo 3.

[191] L. DALLA CORTE, *A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection*, in D. HALLINAN et al. (eds.), *Data Protection and Privacy: Data Protection and Democracy*, Hart Publishing, Oxford, 2020, pp. 27-58.

[192] Sulle forme di controllo presenti nel GDPR, cfr. sezione 3.2 del capitolo 3.

[193] V. sentenza della Corte del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970, punto 129.

umana (art. 1). In aggiunta, secondo le Spiegazioni alla Carta, il diritto alla protezione dei dati personali è fondato – oltre che sull'art. 268 TCE (oggi, art. 16 TFUE), sull'art. 8 della CEDU e della Convenzione 108 – sulla direttiva 95/46/CE (oggi, GDPR), che non prevede un divieto generale di trattamento dei dati [194], ma riconosce esplicitamente, accanto alla componente del diritto fondamentale alla protezione dei dati personali, quella relativa all'uso e alla circolazione degli stessi [195].

Da ultimo, anche la giurisprudenza più recente della Corte sembra avallare tale impostazione, laddove ha affermato che l'art. 8 della Carta "sancisce, al paragrafo 1, il diritto alla protezione dei dati personali, ma impone anche, nel successivo paragrafo 2, che tali dati vengano trattati nel rispetto di determinate condizioni, dal quale dipende la liceità del trattamento in questione" [196]. In questa prospettiva, gli obblighi previsti dal GDPR a carico del titolare trovano un corrispettivo nei diritti attribuiti agli interessati, i quali possono così beneficiate di "un diritto ad un trattamento lecito dei loro dati personali" [197], inteso come corollario del divieto imposto al titolare di procedere a trattamenti in contrasto con le prescrizioni del regolamento.

Le diverse concettualizzazioni del diritto alla protezione dei dati personali e, in particolare, del suo contenuto essenziale [198], non hanno solamente un valore teorico; da esse derivano differenti approcci nel determinare cosa rappresenti un'ingerenza nell'esercizio del diritto fondamentale in questione. Se si opta per una lettura del diritto alla protezione dei dati personali come "*prohibitive right*", sarà difficile ammettere limitazioni ai sensi dell'art. 52, par. 1, Carta [199]. Al contrario, qualora si accolga un'interpretazione di tale

---

[194] Fatta eccezione per l'art. 9, par. 1, GDPR sul trattamento dei dati sanitari che, tuttavia, può essere derogato *ex* art. 9, par. 2, GDPR.

[195] Cfr. Spiegazioni relative alla Carta dei diritti fondamentali, Gazzetta ufficiale dell'Unione europea C 303/17 – 14 dicembre 2007. Sul valore vincolante delle Spiegazioni alla Carta nell'interpretazione dei diritti in essa contenuti, v. J. ZILLER, *Les Fabuleux Destins Des Explications Relatives à la Charte Des Droits Fondamentaux de l'Union Européenne*, in *Chemins d'Europe: Mélanges en l'honneur de Jean-Paul Jacqué*, 2010, pp. 765-781.

[196] Sentenza della Corte del 4 settembre 2025, causa C-655/23, *Quirin Privatbank*, ECLI:EU:C:2025:655, punto 40.

[197] *Ibid*.

[198] Per una ricognizione teorica relativa al concetto di "contenuto essenziale" dei diritti fondamentali, cfr. F. FERRI, *op. cit.*, 2022, pp. 109-112, e i riferimenti dottrinali ivi citati.

[199] Secondo questa disposizione, eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali riconosciuti dalla Carta possono essere previste dalla legge, qualora rispettino il loro contenuto essenziale e, conformemente al principio di proporzionalità, siano necessarie e rispondano a finalità di interesse generale riconosciute dall'Unione o all'esigenza di tutelare i diritti e le libertà altrui. Per un commento sull'art. 52 della Carta, cfr. P. MANZINI, *La portata dei diritti garantiti dalla Carta dell'Unione europea: problemi interpretativi posti dall'art.*

diritto come "*permissive right*", un'interferenza nel suo esercizio potrebbe ritenersi più facilmente legittima *ex* art. 52, par. 1, Carta. Ciò, tuttavia, a condizione che anche il test previsto da quest'ultima disposizione venga applicato in modo più chiaro [200], assicurando maggiore certezza nei casi in cui sia necessario bilanciare il diritto alla protezione dei dati personali con altri diritti previsti dalla Carta.

5. Gli ostacoli alla piena realizzazione della dimensione economica e sociale dello spazio europeo dei dati sanitari

Sebbene, a livello ideale, lo EHDS presenti un innegabile potenziale nel promuovere lo sviluppo di una pluralità di settori strategici dell'Unione, sarebbe intellettualmente poco rigoroso trascurarne i limiti. Per questo motivo, a conclusione del presente capitolo, appare doveroso evidenziare gli ostacoli alla piena realizzazione della dimensione economica e sociale dello EHDS. Alla luce dell'analisi svolta nelle sezioni precedenti, che ha inquadrato tale regolamento all'interno di un più ampio e articolato contesto costituzionale e normativo, questi ostacoli paiono derivare soprattutto dall'assenza – o dal limitato grado – di coordinamento tra le sue disposizioni e quelle di altri atti di

---

52, in L.S. ROSSI (a cura di), *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, Giuffrè, Milano, 2002, pp. 127-138; P. MENGOZZI, *The Judicial Protection of Individual Rights and the Principle of Proportionality after the Lisbon Treaty*, in *CYELS*, 2014, vol. 16, pp. 335-345; S. PEERS, S. PRECHAL, *Article 52 – Scope and interpretation of rights and principles*, in S. PEERS et al. (eds.), *The EU Charter of Fundamental Rights: A Commentary*, OUP, Oxford, 2014, pp. 1455-1521; F. FERRARO, N. LAZZARINI, *Art. 52. portata e interpretazione dei diritti e dei principi*, in R. MASTROIANNI et al. (a cura di), *op. cit.*, 2017, pp. 1058-1085; T. LOCK, *Articles 51-54*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *Commentary on the EU: Treaties and the Charter of Fundamental Rights*, OUP, Oxford, 2019, pp. 2248-2260; K. LENAERTS, *The EU Charter of Fundamental Rights: Scope of Application and Methods of Interpretation*, in V. KRONENBERGER, M.T. D'ALESSIO, V. PLACCO (sous la direction de), *De Rome à Lisbonne: les juridictions de l'Union européenne à la croisée des chemins: mélanges en l'honneur de Paolo Mengozzi*, Bruxelles, 2013, p. 117.

[200] Per un'analisi critica sul modo della Corte di applicare l'art. 52, par. 1, Carta, v. P. VOGIATZOGLOU, P. VALCKE, *op. cit.*, 2022, p. 36 ss., in cui si sottolinea come i giudici invocano raramente le condizioni fissate all'art. 8, parr. 2 e 3, Carta e, quando ciò è accaduto, non è mai stato chiarito il significato dei principi e dei diritti in essi contenuti e nemmeno il rapporto tra questi e l'art. 52, par. 2, Carta. A questo proposito, cfr. anche C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO, *La trasformazione digitale in Europa. Diritti e principi*, Giappichelli, Torino, 2023, p. 22, dove si esprimono perplessità in merito all'"assenza di criteri oggettivi per aclarare i presupposti del bilanciamento e del successivo contemperamento tra situazioni soggettive" (pp. 21-22).

diritto derivato dell'Unione, sia a carattere orizzontale, come il GDPR, l'AIA e il DGA, sia a carattere verticale, come il regolamento sui dispositivi medici (MDR) [201] e la direttiva 2011/24/UE.

A tal fine, le pagine che seguono si propongono di individuare le principali aree di sovrapposizione e frizione tra lo EHDS e il quadro normativo esistente, soffermandosi in particolare su quei profili che, in fase applicativa, potrebbero generare maggiori problemi in termini di certezza del diritto [202]. L'analisi si concentrerà dapprima sulle disposizioni relative all'uso primario dei dati e ai prodotti di sanità digitale (sezione 5.2), per poi esaminare quelle concernenti l'uso secondario dei dati sanitari elettronici (sezione 5.2). Infine, anticipando un tema che sarà sviluppato più diffusamente nella seconda parte del lavoro, verrà richiamato un ulteriore fattore potenzialmente idoneo a pregiudicare il raggiungimento degli obiettivi perseguiti dallo EHDS, ossia il bilanciamento tra i diversi diritti e interessi in gioco nella sua interpretazione e applicazione (sezione 5.3).

5.1. L'uso primario dei dati sanitari

Per quanto riguarda i diritti delle persone fisiche in relazione all'uso primario dei dati sanitari elettronici personali, lo EHDS non introduce innovazioni sostanziali rispetto al quadro delineato dal GDPR [203]. Le sue disposizioni tendono piuttosto a sovrapporsi a quelle del regolamento generale sulla protezione dei dati, sollevando questioni di coordinamento normativo e, conseguentemente, di certezza del diritto [204]. Questa sovrapposizione risulta particolarmente

[201] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio.

[202] Secondo una giurisprudenza consolidata, il principio della certezza del diritto "esige che le norme di diritto siano chiare, precise e prevedibili nei loro effetti, affinché gli interessati possano orientarsi nelle situazioni e nei rapporti giuridici rientranti nell'ordinamento giuridico dell'Unione" (sentenza della Corte del 3 dicembre 2019, *Repubblica ceca c. Parlamento e Consiglio*, causa C-482/17, ECLI:EU:C:2019:1035, punto 148).

[203] È fatto salvo il diritto alla portabilità dei dati (art. 20 GDPR), la cui portata, come evidenziato da Li e Quinn, viene ampliata in modo considerevole (W. Li, P. Quinn, *The European Health Data Space: An Expanded Right to Data Portability?*, in *Comput. Law Secur. Rev.*, 2024, vol. 52, pp. 2-13). Cionondimeno, nel testo finale dello EHDS sono state apportate alcune rilevanti modifiche al riguardo, circoscrivendo l'esercizio di tale diritto ai soli dati desunti contenuti nel formato europeo di scambio delle cartelle cliniche elettroniche (considerando 15 EHDS) e chiarendo che il diritto alla portabilità riguarda unicamente l'uso primario dei dati (art. 7 EHDS). Sul punto, cfr. W. Li, *The Right to Data Portability in the European Health Data Space: A Follow-up*, in *Health&Aging Law Lab*, 2024.

[204] Parere congiunto del Comitato e del Garante europeo della protezione dei dati personali

evidente se si considera che molti dei diritti riconosciuti dallo EHDS potrebbero già essere ricavati da un'interpretazione sistematica del GDPR [205], alla luce di alcuni dei suoi considerando, della Convenzione 108+ [206] e della Dichiarazione sui diritti e principi digitali [207], adattando così le tutele esistenti allo specifico contesto sanitario.

Un esempio emblematico è rappresentato dal diritto dei pazienti di accedere in modo immediato e gratuito ai propri dati sanitari elettronici [208]. Questo diritto può essere desunto da una lettura combinata degli artt. 15, par. 1 [209], e 12, par. 5 [210], GDPR, interpretati alla luce del considerando 59 GDPR, che sottolinea la necessità per l'interessato di "richiedere e, se del caso, ottenere *gratuitamente*, […] l'accesso ai dati", nonché del considerando 63 GDPR, che menziona espressamente il "diritto di accedere ai dati relativi alla salute, ad esempio le cartelle cliniche mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati" [211].

(rispettivamente, EDPB e EDPS) n. 03/2022 sulla proposta di regolamento sullo spazio europeo dei dati sanitari, punti 47 e 50.

[205] Al contrario, questo tipo di operazioni interpretative non sarebbero sufficienti per diritti come quello alla portabilità, rispetto al quale, in ambito sanitario, è necessario non solo ampliare il campo di applicazione in modo da comprendere i dati desunti, ma anche estendere la possibilità di esercitare tale diritto ai trattamenti che si fondano su una base giuridica diversa dal consenso e dal contratto.

[206] Nella spiegazione alla Convenzione 108+ viene fornita un'interpretazione dei diritti delle persone fisiche specifica per i trattamenti di dati sanitari: "*[c]oncerning health data, rights may also be exercised in a different manner than through direct access. They may be exercised, for instance, with the assistance of a health professional when it is in the interest of the data subject, notably to help him/her understand the data or ensure that the data subject's psychological state is appropriately considered when imparting information – in line, of course, with deontological principles*" (par. 74).

[207] Benché non parli in modo esplicito dei diritti delle persone fisiche rispetto all'uso dei loro dati sanitari, tale dichiarazione rappresenta uno strumento utile quale parametro interpretativo di situazioni meritevoli di tutela che concernono il mondo digitale.

[208] Art. 3 EHDS.

[209] Tale disposizione riconosce all'interessato di ottenere dal titolare del trattamento l'accesso ai dati personali.

[210] L'art. 12, par. 5, GDPR stabilisce che le azioni intraprese per fornire l'accesso ai dati non sono subordinate al pagamento di alcun contributo spese da parte dell'interessato, a meno che le richieste di quest'ultimo siano manifestamente infondate o eccessive.

[211] Come vedremo meglio nel capitolo 3, esistono differenze rilevanti tra il diritto di accesso previsto dal GDPR e quello disciplinato dallo EHDS. In particolare, il diritto *ex* art. 15 GDPR deve essere esercitato direttamente dalla persona fisica nei confronti del titolare del trattamento, mentre l'accesso ai sensi dello EHDS avviene tramite specifici servizi di accesso ai dati e riguarda esclusivamente dati sanitari in formato elettronico. Inoltre, mentre il GDPR consente ampie limitazioni al diritto di accesso (art. 23), lo EHDS prevede restrizioni più

In questo senso, assume rilievo anche la direttiva 2011/24/UE, la quale riconosce il diritto di ricevere una cartella clinica, scritta o elettronica, contenente i dati relativi alle cure ricevute [212]. La stessa direttiva prevede inoltre che i pazienti che richiedono di usufruire o beneficiano di assistenza sanitaria transfrontaliera possano disporre di almeno una copia della cartella clinica, o vi possano accedere da remoto "in conformità e senza pregiudizio delle misure nazionali che attuano le norme dell'Unione relative alla tutela dei dati personali" [213]. Tali disposizioni configurano, nel loro insieme, "un vero e proprio diritto ad una cartella clinica […] che, in ragione del carattere sufficientemente chiaro, preciso e incondizionato delle richiamate disposizioni, può essere fatto valere direttamente dal singolo dinanzi ai giudici e alle autorità amministrative nazionali" [214].

Con riferimento alla creazione di un mercato unico per i prodotti di sanità digitale (cartelle cliniche elettroniche e applicazioni per il benessere) [215], i principali punti di contatto riguardano la disciplina dell'MDR e dell'AIA [216]. Lo EHDS impone infatti ai produttori di dispositivi medici e ai fornitori di sistemi di IA ad alto rischio dichiarati interoperabili con le componenti armonizzate dei sistemi di cartelle cliniche elettroniche il rispetto di requisiti essenziali di interoperabilità e delle specifiche comuni che saranno definite mediante atti esecutivi della Commissione [217]. Tuttavia, poiché queste ultime non sono ancora note, il loro impatto sul quadro normativo esistente rimane incerto.

Una prima analisi dei requisiti essenziali elencati all'allegato II dello

---

circoscritte, giustificate unicamente da esigenze legate alla sicurezza del paziente o da considerazioni di natura etica.

[212] Art. 4, par. 2, lett. f), direttiva 2011/24/UE.

[213] Art. 5, lett. b), direttiva 2011/24/UE.

[214] G. Di Federico, S. Negri, *op. cit*., 2019, p. 229.

[215] Per esigenze di semplificazione, le norme dello EHDS sui prodotti di sanità digitale vengono incluse nella parte relativa all'uso primario dei dati sanitari elettronici, pur essendo consapevoli che, nel testo dello EHDS, queste sono trattate nel Capo III e non nel Capo II.

[216] A ragion del vero, qualora tali prodotti siano qualificabili come prodotti connessi o servizi correlati ai sensi dell'art. 2, nn. 5-6, DA, anche i requisiti previsti da quest'ultimo assumono rilievo per i produttori. Ad esempio, le cartelle cliniche elettroniche e i servizi ad esse associati dovranno essere progettati in modo tale da garantire che i dati dei prodotti e dei servizi correlati "siano, per impostazione predefinita, accessibili all'utente in modo facile, sicuro, gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto" (art. 3, par. 1, DA). L'intento è consentire ai pazienti di esercitare il diritto alla portabilità dei dati sanitari contenuti nelle cartelle cliniche elettroniche per uso primario, permettendo al contempo di rendere tali dati disponibili per finalità di ricerca e innovazione. Per un approfondimento sui possibili problemi di coordinamento tra lo EHDS e il DA, cfr. F. Casarosa, F. Gennari, *Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS*, in *EJRR*, 2025, pp. 1-23.

[217] Art. 27, parr. 3-4, EHDS.

EHDS lascia comunque presupporre la presenza di sovrapposizioni, almeno parziali, con quelli già stabiliti dall'MDR e dall'AIA, che impongono ai produttori di software medici e sistemi di IA ad alto rischio l'osservanza di requisiti non solo a carattere generale, ma anche di interoperabilità e di sicurezza [218]. Di conseguenza, l'obbligo di conformarsi a tali normative potrebbe scoraggiare produttori e fornitori dall'investire in questo settore e, in particolare, dal rendere i loro prodotti interoperabili con i sistemi di cartelle cliniche elettroniche. Il rischio concreto è di limitare, fin dall'inizio, le opportunità offerte dall'interazione tra queste tipologie di prodotti, ad esempio in termini di scambio di dati e ottimizzazione dei processi sanitari.

Problemi analoghi si pongono nel caso dei sistemi di cartelle cliniche elettroniche che incorporano sistemi di IA ad alto rischio, come quelle che, oltre a contenere documentazione clinica, includono funzionalità avanzate, tra cui il triage automatizzato [219]. In tali ipotesi, i fornitori saranno tenuti a garantire la conformità sia ai requisiti dell'AIA sia a quelli dello EHDS, con un potenziale aggravio degli oneri normativi. A questo proposito, sebbene lo EHDS preveda procedure di valutazione della conformità volte a ridurre tale carico [220], mediante meccanismi di registrazione semplificata nei database previsti dai diversi regolamenti [221], resta da verificare se tali misure saranno sufficienti a incentivare l'adozione di queste tecnologie.

Un ulteriore profilo problematico riguarda le applicazioni per il benessere. Mentre l'MDR le definisce in negativo, escludendole dall'ambito dei dispositivi medici in quanto non destinate a finalità diagnostiche o terapeutiche, lo EHDS adotta una definizione più ampia, ricomprendendovi i software destinati a fornire informazioni sulla salute personale o cure diverse dalla prestazione sanitaria in senso stretto [222]. Tale ampiezza non elimina il rischio che, in determinate circostanze, queste applicazioni possano essere qualificate come dispositivi medici ai sensi dell'MDR [223], nonostante l'esclusione contenuta nel considerando 19 di tale regolamento.

Inoltre, permane il problema strutturale legato alla discrezionalità del produttore nella definizione della destinazione d'uso del prodotto in questione [224]. Nel caso delle applicazioni per il benessere disciplinate dallo

[218] V., in particolare, i requisiti contenuti agli all. I e II MDR e agli all. IV e VII AIA.

[219] All. II, punto 5, lett. d), AIA.

[220] Considerando 42 EHDS.

[221] DG Sante, *Frequently Asked Questions on the EHDS*, 2025.

[222] Art. 2, par. 2, lett. ab), EHDS.

[223] Regola 11 dell'all. VIII MDR.

[224] Cfr. S. PALMIERI, T. GOFFIN, *A Blanket That Leaves the Feet Cold: Exploring the AI Act Safety Framework for Medical AI*, in *Eur. J Health Law*, 2023, vol. 20, p. 11 ss. sottolineano le implicazioni di tale scelta con riferimento all'MDR e all'AIA.

EHDS, è improbabile che un produttore dichiari l'interoperabilità del proprio prodotto con un sistema di cartelle cliniche elettroniche – e dunque accetti gli obblighi correlati, come quello di etichettatura – oppure che riconosca che si tratta di un software medico. In tale eventualità, infatti, il prodotto rientrerebbe tra i dispositivi medici a medio-alto rischio, soggetti a certificazione ai sensi dell'MDR, con oneri di conformità ben più gravosi.

Benché nel corso dell'iter legislativo dello EHDS siano state avanzate proposte di modifica volte a chiarire i confini tra il nuovo regolamento e altri atti di diritto derivato (in particolare, GDPR, MDR e AIA) [225], la situazione di incertezza normativa avrebbe potuto essere evitata *ab origine*. Ad esempio, anziché adottare un nuovo atto legislativo autonomo per disciplinare l'uso primario dei dati sanitari elettronici, la Commissione sarebbe potuta intervenire chirurgicamente sulla direttiva 2011/24/UE. Seguendo le indicazioni fornite a suo tempo dal Garante europeo della protezione dei dati (EDPS) [226], il legislatore avrebbe potuto integrare il testo della direttiva con disposizioni sui diritti dei pazienti in relazione all'uso primario dei loro dati sanitari e sulle cartelle cliniche elettroniche [227].

Parallelamente, sarebbe stato possibile riformare l'MDR – peraltro recentemente oggetto di una proposta di modifica da parte della Commissione [228] – introducendo requisiti specifici per i dispositivi medici progettati per interagire con le componenti armonizzate dei sistemi di cartelle cliniche elettroniche [229] e includendo le applicazioni per il benessere nella classe di dispositivi medici

---

[225] Si pensi, ad esempio, all'art. 27 e al considerando 52 EHDS riguardanti l'interazione rispettivamente con l'MDR e l'AIA e il GDPR.

[226] Progetto di parere dell'EDPS sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (2009/C 128/03). In questa occasione, il Garante ha rimproverato al legislatore europeo di non aver previsto disposizioni relative alla protezione dei dati sanitari, il cui utilizzo è alla base del funzionamento di applicazioni di sanità elettronica (*e-health*) e di telemedicina, aspetti che, com'è noto, sono affrontati dalla direttiva 2011/24/UE.

[227] Tali integrazioni, però, potrebbero alterare profondamente la natura intrinseca della direttiva 2011/24/UE, la quale si occupa esclusivamente del coordinamento tra Stati in situazioni transfrontaliere. Al contrario, lo EHDS stabilisce un quadro normativo armonizzato anche per le situazioni che non presentano tale carattere.

[228] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2017/745 e (UE) 2017/746 per quanto riguarda la semplificazione e la riduzione degli oneri derivanti dalle norme relative ai dispositivi medici e ai dispositivi medico-diagnostici in vitro, e che modifica il regolamento (UE) 2022/123 per quanto riguarda il sostegno dell'Agenzia europea per i medicinali ai gruppi di esperti sui dispositivi medici e il regolamento (UE) 2024/1689 per quanto riguarda l'elenco della legislazione di armonizzazione dell'Unione di cui al suo allegato I, COM(2025) 1023 final, del 16 dicembre 2025.

[229] Lo stesso dovrebbe avvenire anche per l'AIA rispetto ai sistemi di IA ad alto rischio dichiarati interoperabili con sistemi di cartelle cliniche elettroniche.

a rischio minimo. In questo modo, tali prodotti sarebbero stati assoggettati a un regime di conformità semplificato, basato sulla sola apposizione di un'etichetta, senza il coinvolgimento di organismi notificati.

5.2. L'uso secondario dei dati sanitari

Passando all'uso secondario dei dati sanitari, l'art. 1, par. 3, EHDS stabilisce che le norme dello EHDS non pregiudicano l'applicazione di altri atti giuridici dell'Unione relativi alla condivisione dei dati sanitari elettronici, compreso il GDPR. Sebbene tale clausola non espliciti chiaramente la natura di *lex specialis* dello EHDS rispetto al GDPR [230], il regolamento costituisce di fatto la base giuridica per il trattamento dei dati sanitari elettronici personali ai sensi degli artt. 6, par. 1, e 9, par. 2, GDPR. Lo stesso EHDS specifica infatti che i titolari (*data holders*) sono tenuti a condividere determinate categorie di dati sanitari elettronici (ad es. dati contenuti nelle cartelle cliniche elettroniche) [231], ai sensi degli artt. 6, par. 1, lett. c), e 9, par. 2, lett. g)-j), GDPR [232]. Inoltre, gli organismi responsabili per l'accesso ai dati sono obbligati a rendere disponibili i dati ricevuti dai titolari a chi ne fa richiesta, in conformità con gli artt. 6, par. 1, lett. e) [233], e 9, par. 2, lett. g)-j), GDPR [234].

---

[230] A questo proposito, occorre ricordare che l'ambito di applicazione dello EHDS comprende sia i dati personali sia quelli non personali, in formato elettronico. L'art. 2, par. 2, lett. a-c), EHDS qualifica i primi quali dati relativi alla salute e dati genetici, così come definiti dal GDPR, ma anche come "i dati relativi a determinanti della salute o i dati trattati nell'ambito della prestazione di servizi e di assistenza sanitaria, che sono trattati in formato elettronico". I dati sanitari elettronici non personali, invece, sono definiti in negativo come dati diversi da quelli personali, compresi i dati che sono stati anonimizzati o quelli che non sono mai stati correlati ad alcuna persona fisica.

[231] Nelle categorie minime di dati sanitari elettronici che devono essere messi a disposizione per l'uso secondario rientrano sia i dati sanitari generati in ambito medico (ad es. cartelle cliniche elettroniche o registri di sanità pubblica, dati trattati per la prestazione di assistenza sanitaria o cure assistenziali o a fini di sanità pubblica, ricerca, innovazione), sia i dati generati dalla persona tramite l'uso di dispositivi medici o di applicazioni per il benessere (art. 51 EHDS).

[232] L'art. 6, par. 1, lett. c), GDPR rappresenta il fondamento giuridico per i trattamenti necessari per adempiere a un obbligo legale al quale il titolare del trattamento è soggetto, mentre l'art. 9, par. 2, lett. g)-j), GDPR costituisce la condizione di liceità propria di quei trattamenti di dati "sensibili" (ad es. dati relativi alla salute) necessari per motivi di interesse pubblico rilevante (lett. g), per finalità di medicina preventiva o di medicina del lavoro (lett. h), per motivi di interesse pubblico nel settore della sanità pubblica (lett. i) o a fini di archiviazione nel pubblico interesse, ricerca scientifica/storica o a fini statistici (lett. j).

[233] Ai sensi dell'art. 6, par. 1, lett. e), GDPR, un trattamento è lecito qualora sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

[234] Artt. 55-57 EHDS.

Nonostante i chiarimenti introdotti nelle fasi di negoziazione del regolamento [235], permane tuttavia un significativo deficit di coordinamento normativo tra il meccanismo di accesso ai dati per uso secondario previsto dallo EHDS e la disciplina del trattamento delle categorie particolari di dati personali contenuta nel GDPR. Tale mancanza di coordinamento emerge, in primo luogo, sul piano definitorio, in relazione al rapporto tra la nozione di "uso secondario" dello EHDS e quella di "ulteriore trattamento" ai sensi del GDPR [236]. Sebbene il legislatore abbia chiarito che le finalità di uso secondario devono essere diverse da quelle originarie [237], avvicinando così le due categorie concettuali [238], restano aperte questioni interpretative di rilievo.

In particolare, ci si domanda se, anche per l'uso secondario dei dati sanitari elettronici personali, debba trovare applicazione la regola del GDPR secondo cui non è richiesta una nuova base giuridica per trattamenti ulteriori effettuati per finalità *compatibili* con quelle che hanno giustificato la raccolta dei dati [239]. Qualora si propendesse per una risposta affermativa e si negasse allo EHDS natura di *lex specialis*, l'uso secondario di dati per motivi ritenuti compatibili – ad esempio, la ricerca scientifica, che gode di una presunzione di compatibilità ai sensi del GDPR [240] – potrebbe rientrare nell'ambito di

---

[235] Al riguardo si vedano in particolare le modifiche apportate al considerando 37 della proposta nell'attuale considerando 52 EHDS.

[236] Cfr. parere congiunto EDPB-EDPS n. 03/2022, punto 42 e 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 *Eur. J. Health Law*, 2023, vol. 30, pp. 138-139.

[237] Al contrario, nella proposta originaria della Commissione, l'uso secondario veniva definito come il trattamento dei dati sanitari elettronici per le finalità specificatamente elencate all'art. 53 EHDS (ad es. interesse pubblico nel settore della sanità pubblica o ricerca scientifica). A differenza dell'ulteriore trattamento ai sensi del GDPR (considerando 50 GDPR), non si precisava che tali finalità dovessero essere necessariamente diverse da quelle per cui i dati erano stati inizialmente raccolti. Di conseguenza, non sembrava sussistere una corrispondenza diretta tra i due concetti: qualora i dati sanitari fossero stati raccolti fin dall'inizio per una delle finalità indicate all'art. 53 EHDS, e non nel contesto dell'uso primario, il loro utilizzo successivo non avrebbe potuto qualificarsi come "ulteriore trattamento" ai sensi del GDPR.

[238] Rimane comunque il fatto che nel caso dell'ulteriore trattamento ai sensi del GDPR è lo stesso titolare a riutilizzare i dati per finalità differenti rispetto a quelle originarie. Al contrario, l'uso secondario disciplinato dallo EHDS implica il trasferimento dei dati a soggetti terzi, che li utilizzano sulla base di una specifica autorizzazione.

[239] Art. 6, par. 4, e considerando 50 GDPR (corsivo aggiunto). A questo proposito, nel parere preliminare dell'EDPS si evidenziava la necessità che "*[t]he boundaries of what constitutes a lawful processing and a compatible further processing of the data*" fosse "*crystal-clear for all the stakeholders involved*" (EDPS, *Preliminary opinion n. 8/2020 on European Health Data Space*, p. 9). Con riferimento, invece, alla questione controversa dell'eventuale necessità di individuare una base giuridica anche nei casi in cui operi la deroga al principio di limitazione della finalità, si rinvia alle considerazioni svolte nel capitolo 4, nota 240.

[240] Art. 5, par. 1, lett. b), GDPR.

applicazione esclusivo del GDPR, senza necessità di conformarsi alle procedure previste dallo EHDS.

Analoghe osservazioni possono essere formulate con riferimento al rapporto tra lo EHDS e la disciplina dell'altruismo dei dati sanitari prevista dal DGA [241]. Mentre i trattamenti fondati sull'altruismo dei dati richiedono il consenso dell'interessato *ex* art. 6, par. 1, lett. a) e 9, par. 1, lett. a), GDPR [242], l'uso secondario dei dati disciplinato dallo EHDS può legittimamente basarsi anche su basi giuridiche diverse (ad es. interesse pubblico) [243]. Ne deriva l'esigenza di chiarire in modo puntuale i confini tra le due fattispecie, al fine di evitare incertezza interpretative e potenziali conflitti applicativi.

Ulteriori criticità emergono dall'interazione tra lo EHDS, l'MDR e l'AIA, in particolare con riferimento all'uso secondario dei dati sanitari per finalità di addestramento, validazione e miglioramento di dispositivi medici basati su sistemi di intelligenza artificiale. In questo ambito si manifesta una tensione tra, da un lato, l'impostazione dello EHDS, che promuove la circolazione e il riutilizzo dei dati attraverso meccanismi centralizzati sotto il controllo degli organismi per l'accesso ai dati, e, dall'altro, l'MDR e l'AIA, che fondano i rispettivi regimi di sicurezza e conformità su obblighi stringenti posti in capo al fabbricante in materia di qualità dei dati, gestione del rischio e tracciabilità dell'intero ciclo di vita del prodotto.

In tale contesto, l'accesso a dataset ottenuti mediante le procedure previste dallo EHDS può condizionare in modo significativo le modalità di svolgimento delle procedure di valutazione della conformità. In particolare, il fabbricante potrebbe trovarsi a disporre di un controllo solo parziale sulle caratteristiche dei dati utilizzati e sulla documentazione relativa alla loro origine, completezza e rappresentatività, elementi essenziali per dimostrare il rispetto dei requisiti di sicurezza e prestazione previsti dall'MDR [244] e dall'AIA [245].

---

[241] Art. 2, n. 16, e considerando 45 DGA. Nel testo finale dello EHDS infatti non è più presente una disposizione specifica sull'altruismo dei dati, diversamente dalla proposta della Commissione che, all'art. 40, disciplinava l'altruismo dei dati sanitari, rinviando però sostanzialmente alle norme del DGA.

[242] Considerando 50 DGA.

[243] Anche se precedenti al testo definitivo dello EHDS, alcune interessanti considerazioni sul punto sono state compiute da M. SHABANI, *The Data Governance Act and the EU's Move Towards Facilitating Data Sharing*, in *Molecular Systems Biology*, 2021, vol. 17, n. 3, p. 3; C. KRUESZ, F. ZOPF, *The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU*, in *Eur. Data Protection L. Rev.*, 2021, vol. 7, n. 4, pp. 569-579. Più di recente, invece, cfr. E. EL ASRY, J. MANSNÉRUS, S. LIEDE, *Striking the Balance: Genomic Data, Consent and Altruism in the European Health Data Space*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

[244] Art. 61 MDR.

[245] Art. 10 AIA.

Questo scollamento rischia di tradursi in un aggravio degli oneri regolatori, ulteriormente accentuato dalle ambiguità che caratterizzano il coordinamento tra gli organismi per l'accesso ai dati [246], le autorità di protezione dei dati [247] e gli organismi notificati competenti per la valutazione della conformità [248].

A tali difficoltà si aggiungono le potenziali tensioni derivanti dal diritto di *opt-out* previsto dallo EHDS [249], il quale, pur rafforzando la tutela dei diritti degli interessati, può incidere sulla disponibilità e sulla rappresentatività dei dataset utilizzati per l'addestramento dei sistemi di IA [250]. Una riduzione selettiva dei dati potrebbe infatti compromettere la capacità dei fabbricanti di individuare e correggere bias e di garantire livelli costanti di sicurezza e prestazione nel tempo, con possibili ricadute anche sulle attività di sorveglianza post-commercializzazione richieste dall'MDR [251] e dall'AIA [252]. In questo quadro, deve anche considerarsi che l'attribuzione agli erogatori di assistenza sanitaria del ruolo di titolari dei dati comporta nuovi obblighi [253] che, in assenza di chiari meccanismi di cooperazione, rischiano di interferire con le responsabilità del fabbricante in materia di *post-market surveillance*.

In conclusione, dall'analisi svolta emerge come la situazione di incertezza giuridica derivante da un coordinamento insufficiente tra lo EHDS e altri atti di diritto derivato dell'Unione sarebbe potuta essere evitata (o quantomeno attenuata) in due modi differenti, a seconda che si faccia riferimento alle norme relative all'uso primario o a quelle sull'uso secondario dei dati. Nel primo caso, come già anticipato, sarebbe stato probabilmente preferibile intervenire sul quadro normativo vigente (ad es. GDPR, direttiva 2011/24/UE e MDR), anziché introdurre un nuovo atto normativo, aggiungendo ulteriore complessità a un sistema già caratterizzato da elevata stratificazione normativa. Nel secondo caso, sarebbe invece stato sufficiente garantire un maggiore allineamento e una più chiara coerenza sistematica tra le disposizioni dello EHDS e quelle di altri regolamenti, sia a carattere orizzontale (GDPR, DGA e AI Act) sia a carattere verticale (MDR).

---

[246] Art. 55 EHDS.

[247] Art. 51 GDPR.

[248] Capo IV MDR e Capo III, sezione 4 AIA.

[249] Art. 71 EHDS.

[250] Sull'impatto potenzialmente negativo per la ricerca derivante da un ricorso massivo al diritto di *opt-out*, cfr. P. CERVERA DE LA CRUZ, T. LALOVA-SPINKS, M. SHABANI, *The European Health Data Space: An Opportunity to Strengthen Citizens Rights and Engage Citizens in Health Data Governance*, in *Front. Med.*, 2026, p. 3.

[251] Artt. 83-86 MDR.

[252] Art. 72 AIA.

[253] Art. 60 EHDS.

Tale impostazione appare pienamente in linea con l'esigenza di semplificazione e razionalizzazione recentemente enfatizzata dalla Commissione europea. Nel contesto della proposta nota come *Digital Omnibus* [254], ad esempio, la Commissione mira a una riorganizzazione strutturale del *data legislative acquis* al fine di ridurre gli oneri amministrativi, migliorare la coerenza del quadro regolatorio e sciogliere alcune incertezze applicative emerse nei primi anni di attuazione del DA, del DGA e del GDPR (e non solo). Tra le modifiche più rilevanti in termini di razionalizzazione si colloca l'intenzione della Commissione di abrogare il DGA, trasponendo nel DA – con limitati adattamenti [255] – le discipline sui servizi di intermediazione dei dati e sulle organizzazioni per l'altruismo dei dati. Parallelamente, la Commissione propone di far confluire nel DA anche le norme del DGA sul riuso dei dati detenuti dal settore pubblico e quelle della direttiva *open data*, così da eliminare duplicazioni e divergenze nelle discipline nazionali di recepimento.

5.3. Il cuore della questione: quale bilanciamento tra i diritti e gli interessi in gioco?

Oltre a considerare eventuali modifiche legislative volte a rafforzare il coordinamento tra le norme dello EHDS e quelle contenute in altri atti di diritto derivato, appare opportuno interrogarsi anche su come questa disciplina dovrà essere interpretata una volta pienamente operativa [256]. A questo proposito, e in considerazione delle riflessioni sviluppate nella presente analisi, si ritiene che l'interprete debba valorizzare il nesso di funzionalità tra gli obiettivi perseguiti dal regolamento, al fine di assicurare un bilanciamento equo e coerente tra i diversi diritti e interessi in gioco. Ad esempio, nell'interpretazione delle norme concernenti il meccanismo di autocertificazione per le

[254] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 e delle 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 della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025. Per una lettura critica dell'utilizzo della tecnica legislativa degli "pacchetti normativi", si rinvia ai riferimenti dottrinali citati nell'introduzione, nota 27.

[255] Tra i cambiamenti più significativi si segnala il passaggio da un sistema di registrazione obbligatoria a un sistema volontario per i fornitori di servizi di intermediazione dei dati (di cui viene rivista la definizione), con l'obiettivo esplicito di diminuire gli oneri regolatori a carico degli operatori di minori dimensioni.

[256] Ai sensi dell'art. 105 EHDS, il regolamento diventerà applicabile il 26 marzo 2029, fatta eccezione per alcune disposizioni soggette a un'applicazione progressiva, la cui operatività potrà essere posticipata fino a quattro o sei anni dalla data di entrata in vigore.

cartelle cliniche elettroniche [257] e di etichettatura per le applicazioni per il benessere [258], occorrerà considerare che lo sviluppo di tali prodotti di sanità digitale non solo genera benefici economici per i produttori/sviluppatori, ma comporta anche vantaggi indiretti agli individui e alla collettività, consentendo loro di monitorare le proprie condizioni di salute e di ridurre i tempi di interazione con i professionisti e le strutture sanitarie.

In un settore come quello della sanità digitale, queste operazioni di bilanciamento possono risultare particolarmente complesse per via della dimensione individuale e collettiva dei diritti coinvolti, in particolare il diritto fondamentale alla salute e il diritto alla protezione dei dati personali. Per quanto riguarda il primo, è forse superfluo ricordare che la sua tutela implica, da sempre, la ricerca di un equilibrio tra la protezione dei diritti degli individui e degli interessi della collettività. Un esempio emblematico è offerto dalla direttiva 2011/24/UE, in cui coesistono disposizioni "*strongly individuated, focused on the central value of patient choice*" [259] e norme [260] che dimostrano un'attenzione maggiore a "*collective rights ideas, in particular the need to protect general national health systems from the unbalancing of their collectively determined provisions by individual claims of entitlement*" [261].

---

[257] Artt. 39-41 EHDS.

[258] Art. 47 EHDS.

[259] T. HERVEY, J. MCHALE, *European Union Health Law: Themes and Implications. Law in Context*, CUP, Cambridge, 2015, p. 189. Secondo le A., la parte della direttiva che riguarda propriamente i diritti dei pazienti "*relies strongly on the idea of patients as consumers, endowed with sufficient information to make informed choices about their health care*" (p. 217).

[260] Ad esempio, l'art. 8 sull'assistenza sanitaria che può essere soggetta ad autorizzazione preventiva. Come rilevato da Hervey e McHale, nonostante il titolo della direttiva 2011/24/UE sembri orientato a favore della posizione dei pazienti, in linea con la giurisprudenza della Corte, le sue disposizioni sono tendenzialmente indirizzate a tutelare le esigenze di programmazione e pianificazione degli Stati (T. HERVEY, J. MCHALE, *op. cit*., 2015, p. 185). In senso analogo, G. DI FEDERICO, *op. cit*., 2014, p. 179: sottolinea che la direttiva "*largely codifies the case law of the Court of Justice on Article 56 TFUE but betrays a conservative approach on the part of Member States. Indeed, some of the most controversial judgments have not been transposed into positive law*".

[261] T. HERVEY, J. MCHALE, *op. cit*., 2015, p. 189. Oltre ad alcune delle disposizioni contenute nella direttiva 2011/24/UE, il tentativo di bilanciare i diritti individuali e gli interessi collettivi è evidente anche in altre misure che sono state adottate durante la pandemia da Covid-19, con un'incidenza rilevante sulla tutela della salute e sulla limitazione dell'esercizio di altre libertà fondamentali per proteggere interessi collettivi. Nella raccomandazione (UE) 2020/1475 del 13 ottobre 2020, il Consiglio ha affermato che le misure nazionali volte a limitare la diffusione del virus Covid-19 devono essere circoscritte nella portata e nel tempo, e non devono eccedere rispetto a quanto strettamente necessario per tutelare la sanità pubblica (pp. 3-9). Si suggerisce altresì di assicurare la coerenza tra tali misure e quelle che mirano ad assicurare la libera circolazione delle merci e dei servizi essenziali nel mercato interno attraverso le c.d. corsie verdi (Comunicazione della Commissione del 23 marzo 2020

In questo modo, da un lato viene protetta la dimensione individuale del diritto alla salute, incarnata nel diritto del singolo a ricevere cure mediche in uno Stato diverso da quello di affiliazione [262]; dall'altro viene tutelata la dimensione collettiva del diritto alla salute, espressa nell'interesse dello Stato di affiliazione a fornire trattamenti sanitari di qualità, accessibili su base universale. Le possibili tensioni tra queste due dimensioni – individuale e collettiva – del diritto alla salute vengono esacerbate, con l'avanzare della digitalizzazione della sanità, dalla necessità di rispettare il diritto alla protezione dei dati personali, la cui realizzazione impone, a sua volta, un ulteriore bilanciamento tra il diritto (di controllo) del singolo sui suoi dati personali e l'interesse della collettività a beneficiare del valore di tali dati.

Questo è evidente nel GDPR, che prevede disposizioni volte a garantire il massimo livello di tutela per gli interessati rispetto al trattamento dei dati personali [263], ma consente anche di introdurre limitazioni a tale tutela in presenza di motivi di interesse pubblico [264]. Ad esempio, l'ulteriore trattamento dei dati sanitari ai fini di ricerca è ammesso – almeno in linea di principio – qualora consenta di perseguire finalità relative all'interesse generale e alla salute,

---

sull'attuazione delle corsie verdi, 2020/C 96 I/01). Un altro esempio è rappresentato dal regolamento (UE) 2021/953 del 14 giugno 2021 su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla Covid-19 (certificato Covid digitale dell'UE) per favorire la libera circolazione delle persone durante la pandemia. Secondo tale regolamento, gli Stati membri possono introdurre restrizioni alla libera circolazione delle persone al fine di limitare la diffusione del virus solo sulla base di motivi di interesse pubblico specifici e limitati, nel rispetto del principio di proporzionalità e non discriminazione. Sul punto si rinvia anche alla sentenza della Corte del 5 dicembre 2023, causa C-128/22, *Nordic Info*, ECLI:EU:C:2023:951, analizzata nel capitolo 1, nota 15.

[262] V. conclusioni dell'Avvocato generale Ruiz-Jarabo Colomer in *Stamatelaki*, punto 40. In dottrina, C. NEWDICK, *The European Court of Justice, Transnational Health Care, and Social Citizenship – Accidental Death of a Concept?*, in *Wis. Int. Law J*., 2008, vol. 26, pp. 844-867; T. HERVEY, *The Right to Health in European Union Law*, in T. HERVEY, J. KENNER (eds.), *Economic and Social Rights under the EU Charter of Fundamental Rights: A Legal Perspective*, Hart Publishing, London, 2003, pp. 193-222.

[263] Artt. 6, par. 1, lett. a) e 9, par. 2, lett. a), GDPR.

[264] In particolare, si vedano le eccezioni all'uso dei dati personali relativi alla salute di cui all'art. 9, par. 2, GDPR. Rispetto all'art. 8, par. 3, direttiva 1995/46/CE, che consentiva di derogare al divieto di trattamento dei dati quando fosse "necessario alla prevenzione o alla diagnostica medica, alla somministrazione di cure o alla gestione di centri di cura e quando [… fosse] effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale […] o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente", l'art. 9, par. 2, GDPR introduce l'eccezione relativa al bisogno di "proteggere la popolazione da gravi minacce per la salute a carattere transfrontaliero, ovvero di garantire standard elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici". Art. 9, par. 2, lett. i) e considerando 52 e 54 GDPR.

conformemente al principio di proporzionalità [265]. La previsione di un simile regime derogatorio deriva dalla consapevolezza che l'uso e la condivisione dei dati sono essenziali per il buon funzionamento dei sistemi sanitari [266] e per lo sviluppo di conoscenze fondamentali, ad esempio in relazione all'impatto delle determinanti sociali della salute, come il livello di istruzione o la condizione occupazionale [267].

In linea con questa impostazione, anche lo EHDS si muove su questo duplice piano, ossia quello individuale di tutela delle posizioni soggettive dei pazienti e quello generale connesso alla salvaguardia del benessere collettivo. In particolare, nelle parti dedicate all'uso primario dei dati sanitari elettronici, si coglie lo sforzo di bilanciare il diritto fondamentale degli individui alla protezione dei dati personali, inteso come controllo sui dati contenuti nella cartella clinica elettronica, con il diritto alla salute, che comprende l'accesso a cure di qualità, anche in contesti transfrontalieri. Le norme sui diritti delle persone fisiche rispetto ai loro dati sanitari sono emblematiche di questo bilanciamento.

Lo EHDS riconosce infatti una serie di diritti individuali, come il diritto di accesso ai dati sanitari elettronici [268], il diritto di limitare l'accesso di operatori sanitari e fornitori di assistenza sanitaria ai propri dati [269], e il diritto di *opt-out* all'uso primario [270]. Tuttavia, lo stesso regolamento ammette che l'esercizio di tali diritti possa essere limitato per motivi di sicurezza del paziente o per esigenze etiche [271], oppure per salvaguardare gli interessi vitali del paziente o di altre persone [272]. Sebbene tali eccezioni implichino una compressione del diritto al controllo individuale sui dati, esse mirano in ultima analisi a garantire ai pazienti stessi un migliore accesso all'assistenza sanitaria (nazionale e transfrontaliera), una maggiore qualità ed efficacia in termini di costi dell'erogazione dell'assistenza sanitaria e una modernizzazione dei sistemi sanitari.

Anche per quanto concerne l'uso secondario dei dati, lo EHDS persegue un equilibrio tra il diritto individuale alla protezione dei dati personali e

---

[265] Artt. 9, par. 2, lett. j), e 89 GDPR.

[266] Considerando 53 GDPR.

[267] Considerando 157 GDPR.

[268] Art. 3 EHDS.

[269] Art. 8 EHDS.

[270] Art. 10 EHDS.

[271] Art. 3, par. 3, e considerando 9-10 EHDS. Queste disposizioni consentono agli Stati membri, in conformità con l'art. 23 GDPR, di introdurre restrizioni all'accesso ai dati da parte delle persone fisiche, ad esempio rinviandolo fino a quando un professionista sanitario non sia in grado di fornire adeguate spiegazioni sulle informazioni che potrebbero avere un impatto sulla loro salute.

[272] Artt. 8 e 10 EHDS.

l'interesse di terzi e della collettività a utilizzare tali dati per favorire la ricerca in ambito biomedico e la competitività dell'industria europea, nonché supportare le autorità sanitarie nel prendere decisioni per migliorare l'accessibilità, l'efficacia e la sostenibilità dei sistemi sanitari. Un esempio significativo in tal senso è rappresentato dal diritto di *opt-out* all'uso secondario dei dati [273], il cui esercizio può essere oggetto di restrizioni da parte degli Stati membri in circostanze particolari. Ciò accade, ad esempio, qualora i dati siano richiesti da enti pubblici per finalità di rilevante interesse pubblico e non esistano mezzi alternativi per ottenere tali informazioni in modo tempestivo ed efficace. Queste limitazioni, analogamente a quanto osservato in relazione ai diritti riconosciuti per l'uso primario, trovano giustificazione nella necessità di perseguire obiettivi di interesse generale che mirano a migliorare il benessere collettivo, con effetti positivi anche per l'individuo a cui i dati si riferiscono.

In conclusione, è opportuno sottolineare che lo EHDS, in linea con il GDPR, è stato concepito per favorire l'utilizzo e la condivisione dei dati nel rispetto del diritto fondamentale alla protezione dei dati personali, tenendo conto del valore economico e sociale di tale risorsa per gli individui e la società nel suo complesso. Entrambi i regolamenti prevedono dei meccanismi volti a garantire un equilibrio tra i diritti e gli interessi in gioco. Tuttavia, come approfondiremo nei capitoli 3 e 4, le modalità con cui tale bilanciamento viene realizzato – attraverso l'interpretazione o l'applicazione concreta delle disposizioni normative – risultano determinanti per il raggiungimento effettivo degli obiettivi perseguiti dal legislatore europeo.

6. Riflessioni conclusive

Il presente capitolo ha mostrato come la duplice dimensione dello EHDS consenta di massimizzare il valore dei dati per il raggiungimento di obiettivi strategici dell'Unione, quali la creazione di un mercato unico digitale e il rafforzamento del SER, nel rispetto dei diritti fondamentali dell'Unione (in particolare, il diritto alla salute e alla protezione dei dati personali). Tuttavia, si è anche evidenziato come il potenziale dello EHDS nel raggiungimento di tali obiettivi rischi di essere compromesso da due fattori principali. Da un lato, l'assenza di un adeguato coordinamento tra lo EHDS e altri atti di diritto derivato dell'Unione (*in primis*, il GDPR, l'MDR e l'AIA). Dall'altro, il rischio che le scelte di bilanciamento tra i diversi diritti e interessi coinvolti nell'interpretazione e applicazione dello EHDS, vengano compiute senza una sufficiente

[273] Art. 71 EHDS.

valorizzazione del nesso funzionale tra le sue finalità economiche e sociali, nonché della dimensione individuale e collettiva dei diritti in gioco.

In continuità con queste riflessioni, la seconda parte del lavoro sarà dedicata all'esame del rapporto tra lo EHDS e il GDPR, con l'obiettivo di approfondire le tensioni che possono emergere tra i rispettivi modelli regolatori e le relative implicazioni sul piano del bilanciamento tra la tutela del diritto individuale al controllo sui dati personali e gli interessi di terzi e della collettività. Si cercherà, in particolare, di valutare se tali tensioni possano essere risolte – o quantomeno attenuate – attraverso una rilettura critica delle modalità di interpretazione (capitolo 3) e applicazione (capitolo 4) finora adottate del GDPR, così da rendere possibile una realizzazione piena e armonica degli obiettivi comuni dei due regolamenti.

Parte II

Le tensioni (costituzionali e fisiologiche) tra lo spazio europeo dei dati sanitari e il GDPR

Capitolo 3
L'interpretazione del GDPR alla luce dello spazio europeo dei dati sanitari

"*Ci si trova al cuore della questione del rapporto fra individuo e collettività nella società digitale. Una questione che esige, da un lato, la ricerca e l'attuazione di equilibri delicati fra gli interessi della collettività e i diritti degli individui, prendendo le mosse dall'importanza assoluta che questi ultimi hanno nel patrimonio costituzionale europeo, e, dall'altro, la predisposizione di garanzie contro gli abusi*".

(Pitruzzella, 2022) [1]

Sommario: 1. Premessa. – 2. La tutela degli interessati al centro delle interpretazioni relative alla disciplina europea sui dati personali. – 2.1. L'ambito di applicazione materiale. – 2.2. I mezzi di conciliazione dei diritti e degli interessi in gioco. – 2.2.1. Il diritto di accesso ai dati personali e le possibili limitazioni. – 2.2.2. I dati sensibili e le deroghe al divieto generale di trattamento. – 3. Verso un equilibrio maggiormente in linea con gli obiettivi strategici del legislatore europeo. – 3.1. Le scelte del legislatore nell'ambito dello spazio europeo dei dati sanitari. – 3.1.1. La tutela dei diritti individuali (di controllo). – 3.1.2. I servizi e gli organismi per l'accesso ai dati sanitari elettronici. – 3.2. I cambiamenti necessari nell'interpretazione del GDPR. – 3.2.1. I limiti all'ambito di applicazione materiale. – 3.2.2. Alcune ipotesi alternative di bilanciamento nell'interpretazione dei mezzi di conciliazione. – 4. Riflessioni conclusive.

1. Premessa

Il regolamento sullo EHDS mira a favorire l'uso e la libera circolazione dei dati sanitari elettronici all'interno dell'Unione, al fine di consentire agli individui e alla collettività nel suo complesso di beneficiare del valore economico e

[1] Conclusioni dell'Avvocato generale Pitruzzella del 27 gennaio 2022, causa C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:65, p. 2.

sociale di tali dati [2]. Dal momento che la categoria di "dati sanitari elettronici", ai sensi dello EHDS, comprende anche i dati sanitari personali [3], l'applicazione di tale strumento normativo deve necessariamente fare i conti con il rispetto di quello che il Comitato e il Garante per la protezione dei dati personali (rispettivamente, EDPB e EDPS) definiscono come l'"*acquis* dell'UE nel settore della protezione dei dati" [4]. Ciò significa che il quadro normativo stabilito dallo EHDS non deve pregiudicare la disciplina sulla protezione dei dati personali [5], dovendo essere letto in conformità alla normativa europea in

[2] Sul punto, si rinvia all'analisi svolta nel capitolo 2.

[3] Art. 2, par. 2, lett. c), EHDS. A questo proposito, vale la pena di sottolineare che una netta distinzione tra dati personali e dati non personali è difficilmente operabile. Tale difficoltà deriva non soltanto dall'interpretazione estensiva fornita dalla Corte riguardo alla nozione di "dato personale" (v. sezione 2.1), ma anche dal fatto che, "se le parti di dati personali e di dati non personali sono 'indissolubilmente legate', i diritti e gli obblighi in materia di protezione dei dati derivanti dal regolamento generale sulla protezione dei dati si applicano pienamente all'insieme di dati misti, anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme di dati" (Comunicazione della Commissione al Parlamento e al Consiglio, *Guidance on the Regulation on a Framework for the Free Flow of Non-personal Data in the European Union*, COM(2019) 250 final, del 29 maggio 2019, pp. 5 e 10). In dottrina, tra gli autori che evidenziano la difficoltà nel tracciare una precisa linea di demarcazione tra le due categorie di dati, cfr. N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law Innov. Technol*, 2018, vol. 10, n. 1, p. 40 ss.; B-J. KOOPS, *The Trouble with European Data Protection Law*, in *Int. Data Priv. Law*, 2014, vol. 4, n. 4, p. 250 ss.; M. FINCK, F. PALLAS, *They Who Must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR*, in *Int. Data Priv. Law*, 2020, vol. 10, n. 1, p. 12; C. IRTI, *Personal Data, Non-Personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. SENIGAGLIA, C. IRTI, A. BERNES (eds.), *Privacy and Data Protection in Software Service*, Springer, Singapore, 2022, p. 50. Altri autori ritengono che questa distinzione non solo sia difficile da tracciare, ma sia anche priva di utilità, cfr. I. GRAEF, R. GELLERT, M. HUSOVEC, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation*, in *TILEC Discussion Paper No. 2018-029*, 2018; J. DREXL, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, in A. DE FRANCESCHI, R. SCHULZE (eds.), *Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice*, Beck, München, 2019, p. 19 ss.

[4] Parere congiunto di EDPB-EDPS n. 03/2021 sulla proposta di DGA, punto 19, p. 8 e parere congiunto n. 03/2022 sulla proposta di regolamento sullo spazio europeo dei dati sanitari, p. 6. Nel parere, inoltre, è stato sottolineato come il modello dell'Unione europea sull'integrazione dei valori e dei diritti fondamentali debba necessariamente rappresentare il paradigma nello sviluppo delle politiche europee e che il GDPR debba essere considerato un fondamento sul quale costruire il nuovo sistema di governance europea dei dati.

[5] Art. 1, par. 3, EHDS. Lo stesso viene affermato nel regolamento (UE) 2022/868 sulla governance dei dati (DGA) (considerando 4) e nel regolamento (UE) 2023/2854 sui dati (DA) (considerando 7).

materia di protezione dei dati personali, come interpretata dalla Corte [6].

L'insistenza con cui il legislatore europeo ha affermato che lo EHDS, così come gli altri regolamenti della Strategia europea per i dati, devono "lasciare impregiudicate" le disposizioni del GDPR è sintomatica della centralità che tale disciplina ha ormai assunto nell'ordinamento europeo e non solo. L'introduzione del GDPR ha permesso, infatti, di stabilire un quadro normativo organico a tutela delle persone fisiche riguardo al trattamento dei dati personali, unico nel suo genere, con esempi di emulazione normativa anche fuori dai confini dell'Unione [7]. Allo stesso tempo, l'orientamento giurisprudenziale che si è consolidato sul GDPR, e ancor prima sulla direttiva 95/46/CE (DPD), ha contribuito all'affermarsi di una vera e propria cultura della protezione dei dati personali, fondata su una concezione del diritto fondamentale alla protezione dei dati personali come intrinsecamente connesso al diritto alla riservatezza e alla dignità umana [8].

Per quanto riguarda il trattamento dei dati relativi alla salute, il GDPR, in sostanziale continuità con la DPD, pone un generale divieto di trattamento dei dati c.d. sensibili, tra cui rientrano anche quelli sanitari. Tale divieto può, tuttavia, essere derogato qualora il titolare del trattamento dia prova dell'esistenza di una base giuridica adeguata, ai sensi degli artt. 6, par. 1, e 9, par. 2, GDPR, nonché ottemperi a una serie di adempimenti volti a salvaguardare i diritti e le libertà fondamentali degli individui. Inoltre, il GDPR, sempre per via della natura particolarmente sensibile dei dati sanitari, ammette la possibilità che gli Stati membri mantengano o introducano ulteriori condizioni, comprese limitazioni al trattamento di dati genetici, biometrici e relativi alla salute [9].

---

[6] Parere congiunto di EDPB-EDPS n. 03/2022, p. 7.

[7] Tra i Paesi extra UE che hanno subìto il ruolo catalizzatore del GDPR, introducendo norme sulla protezione dei dati personali, si vedano il *California Consumer Privacy Act* del 2018 e la *Personal Information Protection Law* cinese del 2021. Lo stesso Segretario delle Nazioni Unite António Guterres, nel suo discorso al Senato Italiano del 18 dicembre 2019, ha evidenziato come il GDPR "abbia fissato un esempio [...] che ispira misure analoghe" (disponibile al seguente link: https://www.un.org/press/en/2019/sgsm19916.doc.htm). Sul tema, infine, non può non citarsi il lavoro di A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, OUP, Oxford, 2020.

[8] Secondo l'EDPS, "*[t]he respect for, and the safeguarding of, human dignity could be the counterweight to the pervasive surveillance and asymmetry of power which now confronts the individual. It should be at the heart of a new digital ethics. […] Privacy is an integral part of human dignity, and the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale of personal processing*" (parere dell'EDPS n. 04/2015, Verso una nuova etica digitale. Dati, dignità e tecnologia). Questo aspetto è stato approfondito all'interno del capitolo 2, sezione 4.2.

[9] Art. 9, par. 4, e considerando 10 GDPR. In virtù del margine di manovra riconosciuto agli Stati membri, in Italia, ad esempio, il d.lgs. 30 giugno 2003, n. 196, Codice in materia di

Così come anticipato nel capitolo 2 del presente lavoro [10], lo EHDS rappresenta la norma di "diritto dell'Unione" che costituisce la base giuridica per i trattamenti di dati sanitari *ex* art. 9, par. 2, GDPR, soprattutto per quelli necessari ai fini di interesse pubblico rilevante, cura, interesse pubblico nel settore della sanità pubblica e ricerca scientifica [11]. Dando attuazione alle eccezioni che lo stesso GDPR ammette al divieto di trattamento dei dati relativi alla salute, lo EHDS mira a creare un quadro normativo favorevole all'uso (primario e secondario) e alla libera circolazione dei dati sanitari tra Stati membri, nel rispetto – occorre ribadirlo – dell'*acquis* europeo in materia di protezione dei dati personali.

Per fare ciò, il legislatore europeo si ispira al modello regolatorio del GDPR, fondato sull'attribuzione di diritti (non assoluti) alle persone fisiche e sulla previsione di regole volte a favorire il trattamento legittimo dei dati personali [12], aggiungendo un tassello ulteriore che consiste nell'istituzione di un sistema di governance dei dati a livello nazionale (ad es. i servizi di accesso ai dati e gli organismi per l'accesso ai dati sanitari) e sovranazionale (ad es. le infrastrutture per l'uso primario e secondario dei dati sanitari) [13].

Lo EHDS, quindi, non costituisce una deroga al regime previsto dal

---

protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, ha previsto l'intervento del Garante per la protezione dei dati personali per l'adozione di specifiche misure di garanzia (art. 2-*septies*) e di regole deontologiche (art. 2-*quater*).

[10] Si veda, in particolare, la sezione 5.2 del capitolo 2.

[11] Art. 9, par. 2, lett. g)-j), GDPR.

[12] Come chiarito da una giurisprudenza ormai consolidata della Corte, infatti, "[q]ualsiasi trattamento di dati personali deve rispettare i principi disciplinanti il trattamento di tali dati nonché i diritti dell''interessato'" (v., *inter alia*, sentenza *Quirin Privatbank*, ECLI:EU:C:2025:655, punto 39).

[13] Con "sistema di governance dei dati" si intende l'insieme di meccanismi, intermediari e infrastrutture finalizzati a favorire l'uso sicuro dei dati sanitari elettronici nello EHDS. Questa espressione non va confusa con il termine "governance", che si riferisce invece agli attori istituzionali incaricati di garantire una coerente e uniforme applicazione dello EHDS. A questo proposito, benché la questione esuli dal campo della presente analisi, vale la pena precisare che il sistema di governance previsto dallo EHDS si articola su due livelli: i) nazionale, con l'istituzione di autorità di sanità digitale per l'uso primario (art. 19 EHDS) e di organismi responsabili per l'accesso ai dati per l'uso secondario (artt. 57, par. 1, lett. a), n. ii), 63-65, EHDS); ii) sovranazionale, tramite la creazione del Comitato europeo per lo EHDS (art. 92 e 94 EHDS) e l'attribuzione di compiti specifici alla Commissione (art. 96 EHDS). Per un approfondimento sul tema, si consenta di rimandare all'analisi di A. FIORENTINI, *Alla ricerca di un punto di equilibrio tra autonomia istituzionale ed effettività del diritto per le forme di integrazione amministrativa nel settore digitale*, in *Quaderni AISDUE, Sezione "Atti convegni AISDUE"*, 2023, n. 30, pp. 652-673.

GDPR [14], bensì ne specifica il contenuto e ne garantisce l'effettività in un settore determinato, ossia quello sanitario. Se questo è vero a livello teorico, nella pratica, potrebbe sorgere una tensione costituzionale e fisiologica tra le due discipline: mentre il GDPR si è affermato come regolamento volto prioritariamente alla tutela del diritto individuale alla protezione dei dati personali (art. 8 della Carta), lo EHDS è stato concepito al fine di salvaguardare i diritti dei singoli ad accedere ed esercitare un controllo effettivo sui loro dati sanitari, nonché a favorire il riuso di tali dati a fini di ricerca, sviluppo e innovazione (art. 35 della Carta).

In tal senso, non può escludersi che la nuova disciplina istituisca, *de facto*, un regime derogatorio, specie alla luce di come le norme del GDPR sono state interpretate e attuate. Da un lato, la Corte ha offerto una lettura del GDPR fortemente orientata alla tutela degli interessati, limitando o rendendo più difficile lo svolgimento di attività di trattamento. Dall'altro, i legislatori nazionali, sfruttando il margine di discrezionalità riconosciuto loro, hanno bilanciato in modo diverso i diritti e gli interessi in gioco nell'applicazione del GDPR, creando così un quadro normativo frammentato che ostacola la libera circolazione dei dati personali nell'Unione.

In questa seconda parte del lavoro, evidenzieremo come simili approcci nell'interpretazione e nell'applicazione del GDPR possano costituire un limite al raggiungimento degli obiettivi dello EHDS, pregiudicando, in particolare, l'efficacia delle norme relative all'uso primario e secondario dei dati sanitari elettronici, nonché quelle volte a favorire la libera circolazione dei tali dati nell'Unione. Obiettivi che, come vedremo, sono condivisi – almeno formalmente – dallo stesso GDPR. Mentre nel capitolo 4 ci soffermeremo in modo più dettagliato sugli ostacoli posti dall'applicazione diversificata del GDPR a livello nazionale per lo scambio di dati sanitari tra diversi Stati membri, nel presente capitolo ci concentreremo sul ruolo dell'attività ermeneutica della Corte nella concettualizzazione della disciplina europea dei dati personali come normativa essenzialmente votata alla protezione delle prerogative degli interessati.

In primo luogo, illustreremo i tratti essenziali dell'approccio adottato dai giudici di Lussemburgo nell'interpretare la DPD e il GDPR, evidenziando la forte enfasi posta sulla tutela della posizione giuridica degli interessati piuttosto

[14] La sola deroga esplicita alle disposizioni del GDPR da parte dello EHDS era rappresentata dall'art. 38, par. 2, della proposta di EHDS che esentava gli organismi responsabili dell'accesso ai dati sanitari dall'applicazione dell'art. 14 GDPR sul diritto all'informazione. Tuttavia, durante l'iter legislativo, questa disposizione è stata espunta dal testo dello EHDS, anche in ragione delle aspre critiche ricevute non solo da EDPB e EDPS (parere congiunto n. 03/2022, pp. 9, 12 e 26), ma anche dalla dottrina (*inter alia*, P. TERZIS, *Compromises and Asymmetries in the European Health Data Space*, in *Eur. J. Health Law*, 2023, vol. 30, pp. 360-361).

che su quella dei titolari del trattamento quali portatori di interessi propri o della collettività (sezione 2). In secondo luogo, sottolineeremo come, sebbene lo EHDS si ispiri al modello regolatorio del GDPR e debba rispettare l'*acquis* europeo in materia di protezione dei dati personali, non sia opportuno utilizzare lo stesso approccio interpretativo affermatosi per il GDPR al fine di evitare di compromettere la realizzazione degli obiettivi dello EHDS. Inoltre, alla luce dei recenti sviluppi normativi, ci interrogheremo sulla necessità di ripensare al modo in cui il GDPR è stato interpretato finora, non solo per dare piena realizzazione ai "veri" obiettivi dello stesso, ma anche per assicurare una maggiore coerenza nell'intero ordinamento (sezione 3).

2. La tutela degli interessati al centro delle interpretazioni relative alla disciplina europea sui dati personali

Nell'attività ermeneutica della Corte relativa alla DPD e al GDPR [15], si osserva una chiara propensione a favorire "i diritti personalistici (in particolare, la protezione dei dati personali) in luogo agli interessi del titolare del trattamento e della collettività" [16], derivante dalla scelta di interpretare (teleologicamente) [17] questa disciplina alla luce del (solo) obiettivo di garantire un elevato livello di tutela ai diritti degli interessati. Con alcune differenze tra i casi precedenti e successivi a Lisbona, questo orientamento, da un lato,

[15] La decisione di prendere in considerazione anche la giurisprudenza relativa alla DPD è dettata dal fatto che, in più occasioni, la Corte ha precisato che le norme del GDPR hanno una portata "sostanzialmente identica" a quella delle norme della DPD e, dunque, le interpretazioni relativa a quest'ultima sono, in linea di principio, da considerarsi applicabili anche al GDPR (sentenze della Corte del 7 marzo 2024, causa C-604/22, *IAB Europe*, ECLI:EU:C:2024:214, punto 33 e del 17 giugno 2021, causa C-597/19, *M.I.C.M.*, ECLI:EU:C:2021:492, punto 107).

[16] F. FERRI, *Il bilanciamento tra diritti fondamentali nel mercato unico digitale*, Giappichelli, Torino, 2022, pp. 213-214. In senso analogo, cfr. P. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018, p. 180.

[17] Per via della vaghezza concettuale della disciplina europea per i dati, la Corte fa ampio ricorso al criterio teleologico, come evidenziato da M. TZANOU, *Data Protection as a Fundamental Right Next to Privacy? Reconstructing' a not so New Right*, in *Int. Data Priv. Law*, 2013, vol. 3, n. 2, p. 94; M. TZANOU, *Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection*, in *Croat. Yearb. Eur. Law & Policy*, 2010, vol. 6, n. 6, pp. 59-60; S. GUTWIRTH et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009; P. KUCH, *Teleology: The Missing Piece to Solving the GDPR Puzzle*, in *J. Data Prot. Priv.*, 2021, vol. 5, n. 1, pp. 5-6; S. LINDROOS-HOVINHEIMO, *Who Controls our Data*? *The Legal Reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v. Jehovan todistajat*, in *Inf. Commun. Technol. Law*, 2019, vol. 28, p. 226.

determina un'estensione del campo di applicazione *ratione materiae* della normativa (sezione 2.1) [18] e, dall'altro, pone il diritto individuale alla protezione dei dati personali in una posizione privilegiata nelle operazioni di bilanciamento con altri diritti e interessi in gioco (sezione 2.2).

2.1. L'ambito di applicazione materiale

Fino a Lisbona, la Corte è stata cauta nell'offrire interpretazioni da cui emergesse l'importanza del diritto previsto all'art. 8 della Carta per la disciplina in materia di protezione dei dati personali. Durante questa fase, fanno eccezione due sentenze "integrazioniste" (*Lindqvist* e *Rundfunk*), con cui la Corte ha dichiarato che la circostanza secondo la quale un trattamento di dati personali non ha alcun impatto sulle libertà fondamentali del mercato non preclude l'applicazione della DPD [19]. Secondo i giudici, infatti, la base giuridica della DPD (art. 110A TCE, oggi art. 114 TFUE) non richiede di valutare caso per caso se il trattamento in questione incida o meno sulla libera circolazione dei dati personali [20]. Per questo motivo, è stato possibile riconoscere come rientranti nell'ambito di applicazione di tale normativa attività che non presentano alcun rapporto con l'instaurazione e il funzionamento del mercato interno, quali la pubblicazione su un sito *online* di dati personali a titolo di

[18] In questa sede non verrà affrontato il tema dell'ampiezza del campo di applicazione soggettivo e territoriale del GDPR. Per un'analisi complessiva sull'espansione della disciplina europea sulla protezione dei dati personali, v. M. BRKAN, *The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?*, in *MJ*, 2016, vol. 23, n. 5, pp. 812-841. Per un approfondimento, invece, sull'estensione territoriale della normativa europea sui dati personali, si rinvia, in giurisprudenza, alle sentenze della Corte del 13 maggio 2014, causa 131/12, *Google Spain*, ECLI:EU:C:2014:317, punti 50-53 e 58 e del 1° ottobre 2015, causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639, punti 25 e 30; in dottrina, a A. BRADFORD, *op. cit.*, 2020, p. 232; S. HENSELER, A. TAMÒ-LARRIEUX, *Reaching Beyond Its Territory – An Analysis of the Extraterritorial Scope of European Data Protection*, in E. KOSTA, R. LEENES, I. KAMARA, *Research Handbook on EU Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022, p. 290 ss.; B. GREZE, *The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives*, in *Int. Data Priv. Law*, 2019, vol. 9, n. 2, pp. 109-128; D.J.B. SVANTESSON, *Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Sport Undermining the Regulation, in Int. Data Priv. Law*, 2015, vol. 5, n. 11, pp. 226-234; G. GREENLEAF, *The Influence of European Data Privacy Standards Outside Europe*, in *Int. Data Priv. Law*, 2012, vol. 2, n. 2, p. 152; C. KUNER, *Data Protection Law and International Jurisdiction on the Internet*, in *Int. J. Law Inf. Technol.*, 2010, vol. 18, n. 2, pp. 176-193.

[19] O. LYNSKEY, *The Foundations of EU Data Protection Law*, OUP, Oxford, 2015, p. 54.

[20] Sentenze della Corte del 6 novembre 2003, causa C-101/01, *Lindqvist*, ECLI:EU:C:2003:596, punti 40 e 42; del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, *Rundfunk*, ECLI:EU:C:2003:294, punto 41.

volontariato [21] e lo svolgimento di compiti di controllo da parte di un organo statale [22].

Una valutazione differente viene invece operata dall'Avvocato generale Tizzano. In entrambe le situazioni sopra menzionate, egli ha escluso l'applicabilità della DPD [23], dal momento che quest'ultima ha come obiettivo principale di favorire la libera circolazione dei dati personali, in quanto fondamentale per il mercato interno, e non invece di salvaguardare i diritti fondamentali, tra cui il diritto alla vita privata [24]. Come evidenziato, la Corte, discostandosi dall'opzione interpretativa suggerita dall'Avvocato generale, ha preferito adottare un'interpretazione del campo di applicazione della DPD che consentisse di riconoscere, al di là della base giuridica dell'atto, la dimensione legata ai diritti fondamentali, oltre che quella economica [25].

Sebbene queste decisioni siano state classificate come "eccezioni" rispetto all'orientamento della Corte nel periodo precedente a Lisbona [26], è evidente che siano gradualmente diventate la "regola" nel periodo successivo [27]. Con il Trattato di Lisbona, infatti, non solo la Carta assume lo stesso valore giuridico dei Trattati [28], ma viene anche introdotto un fondamento normativo *ad hoc* per la protezione e la libera circolazione dei dati personali (art. 16, par. 2, TFUE) [29]. Questi cambiamenti nel quadro costituzionale europeo hanno favorito il consolidarsi di un orientamento interpretativo che estende il campo di applicazione della DPD e, successivamente, del GDPR, al fine di garantire

---

[21] Sentenza *Lindqvist*, punto 48.

[22] Sentenza *Rundfunk*, punti 45-47.

[23] Conclusioni dell'Avvocato generale Tizzano del 19 settembre 2002, causa C-101/01, *Lindqvist*, ECLI:EU:C:2002:513, punto 41 e del 14 novembre 2002, cause riunite C-465/00, C-138/01 e C-139/01, *Rundfunk*, ECLI:EU:C:2002:662, punti 45-48.

[24] Conclusioni dell'Avvocato generale in *Lindqvist*, punti 40-42 e in *Rundfunk*, punti 52-54.

[25] Prima relazione della Commissione sull'attuazione della direttiva sulla protezione dei dati (95/46/CE), COM(2003) 265 final, del 15 maggio 2003, p. 4.

[26] Tra le altre, si rinvia alle sentenze della Corte del 19 aprile 2012, causa C-461/10, *Bonnier*, ECLI:EU:C:2012:219; del 29 gennaio 2008, causa C-275/06, *Promusicae* e del 16 dicembre 2008, causa C-73/07, *Satakunnan Markkinapörssi e Satamedia*, ECLI:EU:C:2008:727.

[27] T. HERVEY, J. MCHALE, *Health Law and the European Union*, OUP, Oxford, 2004, p. 167 che sottolineano che "*even though the internal market and fundamental rights rationales were equally present in the DPD, the fundamental rights rationale turned out to be more powerful in the long run*".

[28] Cfr. L.S. ROSSI, *Same Legal Value as the Treaties? Rank, Primacy, and Direct Effects of the EU Charter of Fundamental Rights*, in *Ger. Law J.*, 2017, vol. 18, p. 771 e L. DANIELE, *Carta dei diritti fondamentali dell'Unione europea e Trattato di Lisbona*, in *DUE*, 2008, vol. 13, p. 655.

[29] Per un commento alla disposizione in esame, si rimanda alla sezione 3.2 del capitolo 1 e, in particolare, alla nota 142.

una tutela ampia alla posizione giuridica degli individui e del loro diritto fondamentale alla protezione dei dati personali [30].

Tale approccio emerge chiaramente dalla giurisprudenza che si è sviluppata attorno alle nozioni di "trattamento" e "dato personale", le cui definizioni sono cruciali per delineare i contorni dell'ambito di applicazione materiale della normativa in questione [31]. Relativamente a entrambi questi concetti, la Corte ha individuato una vasta gamma di tipologie di attività e dati personali che possono rientrare nelle definizioni previste *ex lege*.

Per quanto riguarda il concetto di "trattamento", partendo da un'analisi testuale dell'art. 4, par. 2, GDPR, la Corte ha sottolineato che la scelta di definire il trattamento di dati personali come "*qualsiasi* operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali" riflette la volontà legislativa di attribuire un'accezione ampia a questa nozione [32]. Secondo i giudici, tale scelta è corroborata dall'utilizzo della congiunzione "come" a introduzione di un elenco non tassativo di ipotesi di trattamento (ad es. raccolta e comunicazione mediante trasmissione) [33], ed è suffragata dall'obiettivo del GDPR di assicurare l'effettività del diritto fondamentale alla protezione dei dati personali [34].

Inoltre, nel verificare se una certa operazione qualificabile come trattamento di dati rientra nell'ambito di applicazione del GDPR, la Corte, confermando l'orientamento precedente all'entrata in vigore del Trattato di Lisbona, ha fornito interpretazioni restrittive delle eccezioni all'ambito di applicazione

---

[30] Anche se non circoscritto al settore oggetto della presente analisi, questo fenomeno è stato esaminato da S. IGLESIAS SANCHEZ, *The Court and the Charter: The Impact of the Entry into Force of the Lisbon Treaty on the ECJ's Approach to Fundamental Rights*, in *CMLRev.*, 2012, vol. 49, p. 1566.

[31] Art. 2 GDPR.

[32] Sentenze della Corte del 7 marzo 2024, causa C-740/22, *Endemol Shine Finland Oy*, ECLI:EU:C:2024:216, punti 29-31; del 5 dicembre 2023, causa C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos*, ECLI:EU:C:2023:949, punti 50-51; del 5 ottobre 2023, causa C-659/22, *Ministerstvo zdravotnictví (Applicazione mobile Covid-19)*, ECLI:EU:C:2023:745, punti 27-30; del 24 febbraio 2022, causa C-175/20, *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, EU:C:2022:124, punto 38; del 10 luglio 2018, causa C-25/17, *Jehovan todistajat*, EU:C:2018:551, punto 51; del 6 ottobre 2015, causa C-362/14, *Schrems I*, EU:C:2015:650, punto 45; dell'11 dicembre 2014, causa C-212/13, *Ryneš*, EU:C:2014:2428, punto 25; *Google Spain*, punto 28; *Bonnier Audio e a.*, punto 52.

[33] Sentenze *Endemol Shine*, punto 29; *Ministerstvo zdravotnictví (Applicazione mobile Covid-19)*, punto 27; *Pankki S*, punto 46; *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punto 35.

[34] Sentenze *Endemol Shine*, punto 31 e *Ministerstvo zdravotnictví (Applicazione mobile Covid-19)*, punto 28.

della disciplina europea sui dati personali, che escludono i trattamenti: i) non automatizzati di dati che non sono contenuti in un archivio [35]; oppure effettuati: ii) per l'esercizio di attività che non rientrano nel campo di applicazione del diritto dell'Unione; iii) dagli Stati membri nell'esercizio di attività che rientrano nell'ambito della PESC; iv) da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; v) dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali [36].

Tra le numerose sentenze pronunciate sul punto [37], *Endemol Shine* permette di illustrare in modo esemplare l'approccio della Corte [38]. In questo caso, i giudici hanno riconosciuto la possibilità che una comunicazione orale di dati personali rappresenti un trattamento, non solo perché l'art. 4, par. 2, GDPR menziona espressamente come esempio di trattamento dei dati la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione [39], ma anche perché – pur non essendo un trattamento

---

[35] Art. 3, par. 1, DPD e art. 2, par. 1, GDPR.

[36] Art. 2, par. 2, lett. a)-d), GDPR. La DPD si limitava a escludere solamente i trattamenti effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario (art. 3, par. 2, primo trattino, DPD) e quelli effettuati da una persona fisica per l'esercizio di attività di carattere esclusivamente personale e domestico (art. 3, par. 2, primo trattino, DPD).

[37] Per quanto riguarda le eccezioni contenute nella DPD, v. sentenze *Buivids*, punto 41, *Jehovan todistajat*, punto 37 e del 27 settembre 2017, causa C-73/16, *Puškár*, EU:C:2017:725, punto 38 (sull'art. 3, par. 2, primo trattino, DPD) e sentenza *Ryneš*, punto 29 (sull'art. 3, parr. 1 e 2, secondo trattino, DPD). Con riferimento, invece, al GDPR, v. sentenze *Endemol Shine*, punto 39; *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punto 40 (sull'art. 2, par. 1, GDPR); sentenze della Corte del 16 gennaio 2024, causa C-33/22, *Österreichische Datenschutzbehörde c. WK*, ECLI:EU:C:2024:46, punto 37, del 5 giugno 2023, causa C-204/22, *Commissione europea c. Repubblica di Polonia*, ECLI:EU:C:2023:442, punto 316, del 21 giugno 2022, causa C-817/19, *Ligue des droits humains ASBL*, ECLI:EU:C:2022:491, punto 70, del 22 giugno 2021, *Latvijas Republikas Saeima (Punti di penalità)*, punto 62, *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punto 40 e del 9 luglio 2020, causa C-272/19, *Land Hessen*, EU:C:2020:535, punto 68 (sull'art. 2, par. 2, lett. a), GDPR); sentenza del 22 giugno 2021, causa C-439/19, *Latvijas Republikas Saeima (punti di penalità)*, EU:C:2021:504, punto 64 (sull'art. 2, par. 2, lett. a) e b), GDPR); sentenze *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punti 40-41 e del 21 giugno 2022, causa C-817/19, *Ligue des droits humains ASBL*, ECLI:EU:C:2022:491, punto 70 (sull'art. 2, par. 2, lett. d), GDPR).

[38] Il caso di specie riguarda una richiesta presentata oralmente dalla società Endemol Shine al Tribunale di primo grado del Savo meridionale in Finlandia. La richiesta mirava a ottenere informazioni su eventuali condanne penali in corso o già scontate da parte di una persona fisica partecipante a un concorso organizzato dalla società, al fine di accertare i precedenti giudiziari di tale persona.

[39] Sentenza *Endemol Shine*, punto 33.

automatizzato – le informazioni comunicate oralmente potrebbero rientrare all'interno di un archivio. Questa verifica spetta al giudice del rinvio, il quale, però, deve tenere conto del fatto che la nozione di "archivio" deve essere interpretata in senso ampio per garantire che la tutela conferita dal GDPR alle persone i cui dati sono trattati non dipenda dalle tecniche utilizzate, e per evitare rischi gravi di elusione di tale tutela [40].

Passando alla nozione di "dato personale", la Corte, così come per il "trattamento", parte solitamente dall'analisi testuale dell'art. 4, par. 1, GDPR evidenziando la sintomaticità della scelta del legislatore che, ricorrendo all'espressione "*qualsiasi* informazione", esprime la volontà di conferire un'accezione ampia a tale concetto [41]. Quest'ultimo comprende "potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse 'riguardino' la persona interessata" [42]. A questo proposito, i giudici di Lussemburgo – allineandosi alla

[40] *Ibid.* punto 37.

[41] Tra le altre, si rinvia alla sentenza della Corte del 4 settembre 2025, causa C-413/23, *EDPS c. CRU*, ECLI:EU:C:2025:645, punto 54 (commenti forniti da *stakeholders* e da creditori nell'ambito di una procedura di risoluzione); del 7 marzo 2024, *OC c. Commissione*, C-479/22 P, ECLI:EU:C:2024:215, punto 45 (informazioni contenute in un comunicato stampa); del 4 ottobre 2024, causa C-200/23, *Agentsia po vpisvaniyata*, ECLI:EU:C:2024:827, punti 130-136 (firma autografa); sentenza *IAB Europe*, punto 51 (serie di segni che rivela le preferenze di un utente sul trattamento dei suoi dati); sentenza della Corte del 9 novembre 2023, causa C-319/22, *Scania*, ECLI:EU:C:2023:837 (numeri di identificazione dei veicoli); sentenza *Ministerstvo zdravotnictví (Applicazione mobile Covid-19)*, punti 25 e 28 (dati raccolti con applicazione mobile); del 22 giugno 2023, causa C-579/21, *Pankki S*, ECLI:EU:C:2023:501, punti 41-45 (informazioni relative a operazioni di consultazione dei dati personali); del 4 maggio 2023, causa C-487/21, *Österreichische Datenschutzbehörde e CRIF*, EU:C:2023:369, punto 23 (informazioni relative ai destinatari dei dati personali); *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punti 18 e 34 (informazioni concernenti un autoveicolo messo in vendita, nonché il numero di telefono del venditore di tale autoveicolo); del 22 giugno 2021, causa C-439/19, *B (Punti di penalità)*, EU:C:2021:504, punto 60 (informazioni riguardanti i punti di penalità, che si riferiscono a una persona fisica individuata); del 14 febbraio 2019, causa C-345/17, *Buivids*, EU:C:2019:122, punto 32 (immagini registrate da una telecamera); del 20 dicembre 2017, causa C-434/16, *Nowak*, EU:C:2017:994, punti 36 e 42 (risposte scritte fornite da un candidato a un esame professionale e relative annotazioni dell'esaminatore); del 9 marzo 2017, causa C-398/15, *Manni*, EU:C:2017:197, punto 34 (nome e cognome); *Ryneš*, EU:C:2014:2428, punto 22 (immagine di una persona registrata da una telecamera se ed in quanto essa consente di identificare la persona interessata); del 17 luglio 2014, causa C-141/12 e C-372/12, *Y S e Minister voor Immigratie, Integratie en Asiel*, EU:C:2014:2081, punto 38 (data di nascita, cittadinanza, sesso, etnia, religione e lingua parlata da una persona identificabile attraverso il suo nome); del 30 maggio 2013, causa C-342/12, *Worten*, EU:C:2013:355, punto 19 (dati contenuti in un registro dell'orario di lavoro relativi, per ciascun lavoratore, ai periodi di lavoro giornalieri nonché ai periodi di riposo).

[42] Sentenze *IAB Europe*, punto 36 e giurisprudenza citata.

giurisprudenza relativa alla DPD [43], a sua volta ispirata all'orientamento interpretativo fornito nel parere del Gruppo di lavoro Articolo 29 (WP) [44] – hanno dichiarato che: i) un'informazione riguarda una persona fisica quando, in base al suo contenuto, alla sua finalità o al suo effetto, è connessa a una persona identificabile [45]; ii) una persona è identificabile quando può essere identificata non solo direttamente, ma anche indirettamente, utilizzando informazioni supplementari di cui il titolare del trattamento dispone o potrebbe disporre avvalendosi di mezzi ragionevoli [46].

In base a tali principi, è stato affermato, ad esempio, che perfino una stringa di lettere e caratteri, che rivela le preferenze di un utente di Internet in merito al consenso al trattamento dei propri dati, può costituire un dato personale. Pur non contenendo di per sé elementi che permettono l'identificazione dell'interessato, essa può comunque assumere tale qualificazione qualora, associata a informazioni supplementari (ad es. l'indirizzo IP del dispositivo dell'utente), consenta di risalire alla sua identità [47]. In proposito, i giudici hanno precisato che è irrilevante stabilire se il destinatario dei dati

---

[43] Sentenza *Nowak* e sentenza del 19 ottobre 2016, causa C-582/14, *Breyer*, EU:C:2016:779.

[44] Parere del WP n. 04/2007 sul concetto di dato personale, WP136.

[45] Sentenza della Corte del 4 settembre 2025 (Prima Sezione), causa C-413/23, *EDPS c. CRU*, ECLI:EU:C:2025:645, punto 49; del 4 maggio 2023, causa C-487/21, *Österreichische Datenschutzbehörde e CRIF*, ECLI:EU:C:2023:369, punti 23-24.

[46] Sentenza *IAB Europe*, punti 38-39.

[47] *Ibid.* punti 43-44. Il caso di specie riguarda IAB Europe, un'associazione belga senza scopo di lucro che rappresenta a livello europeo le imprese del settore dell'industria della pubblicità e del *marketing* digitali (ad es. editori, imprese di commercio elettronico e di *marketing*, intermediari, associazioni nazionali). Per favorire il rispetto del GDPR da parte di fornitori di siti Internet o di applicazioni, nonché di broker di dati e piattaforme pubblicitarie, la IAB Europe offre ai suoi membri il *Transparency & Consent Framework* (TCF). Nell'ambito del TCF è stata introdotta la *Consent Management Platform*, ossia un sistema che registra le preferenze degli utenti quando questi, nel consultare un sito Internet o un'applicazione con spazi pubblicitari, decidono se acconsentire o opporsi al trattamento dei propri dati personali per fini specifici come il *marketing* o la pubblicità. Queste preferenze vengono registrate e conservate nella *Transparency & Consent String* (TC String) e successivamente condivise con broker di dati personali e piattaforme pubblicitarie, in modo che questi possano sapere a quali trattamenti l'utente ha prestato il proprio consenso e a quali si è opposto, agevolando così la vendita di pubblicità personalizzata. Dopo aver ricevuto diverse denunce sulla conformità del TCF al GDPR, l'autorità belga di controllo ha adottato una decisione che obbligava la IAB Europe, in qualità di titolare del trattamento di dati personali riguardo alla registrazione delle preferenze degli utenti, a rendere conforme il trattamento dei dati personali effettuato nell'ambito del TCF alle disposizioni del GDPR. Tale decisione è stata poi impugnata da IAB Europe davanti alla Corte d'Appello di Bruxelles, chiedendone l'annullamento. In particolare, venivano contestate la qualifica di IAB Europe come titolare del trattamento e la classificazione della TC String come dato personale.

disponga già delle informazioni aggiuntive necessarie: è infatti sufficiente che egli abbia a disposizione "mezzi ragionevoli" necessari per effettuare l'identificazione [48].

Secondo la Corte, dunque, anche dati "di per sé impersonali", come la stringa sopra menzionata [49], gli indirizzi IP dinamici [50] o le informazioni relative a veicoli [51], possono essere qualificati come personali quando: i) il titolare ha gli "strumenti giuridici" per ottenere da terzi le informazioni aggiuntive che consentono la re-identificazione [52]; oppure ii) il titolare comunica tali dati a soggetti che, a loro volta, possiedono "mezzi che consentano con ragionevole probabilità l'identificazione dell'interessato". In tali casi i dati diventano personali non solo per chi li riceve, ma anche, indirettamente, per lo stesso titolare del trattamento [53].

Infine, l'interpretazione estensiva della nozione di dato personale, corroborata dalle scelte lessicali compiute dal legislatore e finalizzata ad assicurare un regime di tutela elevato alle persone fisiche, è stata applicata, *a fortiori*, ai c.d. dati sensibili [54], inclusi quelli relativi alla salute. Nella sentenza *Vyriausioji tarnybinės etikos komisija* [55], la Corte ha stabilito che rientrano nelle "categorie speciali di dati personali" tutti quei dati che, sebbene non intrinsecamente sensibili, sono in grado di svelare "*indirettamente*, al termine di

---

[48] *Ibid.* punti 46-49.

[49] Sentenza *IAB Europe*, punti 43 e 48.

[50] Sentenza *Breyer*, punti 44, 47 e 48.

[51] Sentenza *Scania*, punti 46 e 49.

[52] Corte del 4 settembre 2025, causa C-413/23, *EDPS c. CRU*, ECLI:EU:C:2025:645, punto 83.

[53] *Ibid.* punto 84. Come si vedrà nella sezione 3.2.1, nella sentenza *EDPS c. CRU*, la Corte ha ribadito l'orientamento già espresso in *OC c. Commissione*, precisando che non può ritenersi ragionevole avvalersi di un mezzo di identificazione quando l'individuazione dell'interessato sia vietata dalla legge oppure risulti, in concreto, praticamente irrealizzabile, ad esempio perché comporterebbe un dispendio sproporzionato di tempo, costi e manodopera.

[54] Considerando 10 GDPR.

[55] Sentenza del 1° agosto 2022, causa C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601. La causa trae origine dalla controversia tra OT e la Commissione principale per la prevenzione dei conflitti di interessi nel servizio pubblico in Lituania (Commissione principale). Quest'ultima ha adottato una decisione in cui contesta a OT, ente percettore di fondi strutturali dell'Unione e provenienti dal bilancio dello Stato lituano, l'inadempimento dell'obbligo di presentare una dichiarazione di interessi privati, previsto dalla legge lituana sulla conciliazione di interessi, che deve essere pubblicata sul sito Internet della Commissione superiore. OT ha impugnato questa decisione, sostenendo di non rientrare tra le persone soggette all'obbligo di dichiarazione degli interessi privati e argomentando che la pubblicazione della dichiarazione potrebbe ledere il suo diritto alla privacy, nonché quello delle altre persone che sarebbe tenuto a menzionare nella propria dichiarazione (ad es. coniuge, convivente o partner).

un'operazione intellettuale di deduzione o di raffronto, informazioni di tale natura" [56]. Tale decisione è stata raggiunta innanzitutto escludendo che il legislatore abbia voluto fare una distinzione all'interno della categoria dei dati sensibili di cui all'art. 9, par. 1, GDPR tra quelli che "rivelino" l'origine razziale o etnica – termine che potrebbe suggerire che i dati siano qualificabili come sensibili anche se non intrinsecamente tali – e quelli "relativi" alla salute o all'orientamento sessuale – termine che invece sembrerebbe implicare l'esistenza di un collegamento più diretto tra i dati personali e l'interessato. Secondo la Corte, questa distinzione non è coerente con una lettura contestuale delle disposizioni del GDPR, dove i dati "relativi" alla salute, ad esempio, vengono definiti come dati attinenti allo stato di salute fisica o mentale di una persona fisica che "rivelano" informazioni concernenti la sua salute.

Inoltre, in linea con l'approccio già adottato in *Lindqvist* con riferimento alla nozione di dati di natura delicata contenuta nella DPD [57], questa distinzione sarebbe contraria all'obiettivo del GDPR (garantire un elevato grado di tutela dei diritti e delle libertà fondamentali delle persone fisiche) e, in particolare, dell'art. 9 GDPR (assicurare una protezione maggiore contro i trattamenti che possono costituire un'ingerenza particolarmente grave nei diritti fondamentali di cui agli artt. 7 e 8 della Carta) [58]. Un'interpretazione più restrittiva dei dati sensibili, dunque, equivarrebbe a sottrarre i trattamenti di questi ultimi al "regime di protezione rafforzato" previsto dal GDPR, pregiudicando "l'effetto utile di tale regime e la tutela dei diritti e delle libertà fondamentali delle persone fisiche che esso mira ad assicurare" [59].

Seguendo questo orientamento, nella sentenza *Lindenapotheke*, la Corte ha riconosciuto come "dati relativi alla salute" le informazioni fornite dai clienti di una farmacia che vende medicinali senza obbligo di prescrizione tramite una piattaforma online (ad es. il nome, il cognome, l'indirizzo di consegna e

---

[56] *Ibid.* punto 123 (corsivo aggiunto). Nel caso di specie, la Corte ha classificato come sensibili "dati personali idonei a divulgare *indirettamente* l'orientamento sessuale di una persona fisica" (punto 128 – corsivo aggiunto). Secondo la Corte, se da tali dati è possibile ricavare, "mediante un'operazione intellettuale di collegamento o di deduzione", informazioni sullo stato di salute di una persona, allora questi devono considerarsi dati relativi alla salute (punto 120). Similmente, cfr. sentenze della Corte del 5 giugno 2023, causa C-204/21, *Commissione c. Repubblica di Polonia (Indipendenza e vita privata dei giudici)*, EU:C:2023:442, punto 344; del 2 dicembre 2025, causa C-492/23, *Russmedia Digital*, ECLI:EU:C:2025:935, punto 52.

[57] Sentenza *Lindqvist*, punto 50. Sulla definizione estensiva dei "dati relativi alla salute", si veda anche la sentenza del Tribunale del 3 dicembre 2015, causa T-343/13, *CN c. EDPS*, ECLI:EU:T:2015:926, punto 50. Tuttavia, in questa occasione, viene sottolineato che tale "nozione non può essere ampliata sino a inglobare espressioni che non comportino la divulgazione di nessun dato relativo alla salute o alla condizione medica di una persona".

[58] Sentenza *Vyriausioji tarnybinės etikos komisija*, punti 122-126.

[59] *Ibid.* punto 127.

altri elementi necessari all'individualizzazione dei medicinali). Secondo i giudici, tali informazioni permettono, attraverso un'operazione di raffronto o di deduzione, di desumere dettagli sullo stato di salute di chi effettua l'ordine, in virtù del legame che si instaura tra "un medicinale, le sue indicazioni o i suoi usi, e una persona fisica identificata o identificabile da elementi quali il nome di tale persona o l'indirizzo di consegna" [60]. La qualificazione di queste informazioni come "dati relativi alla salute" non viene meno per il fatto che i medicinali in questione non richiedono prescrizione, poiché, per la Corte, ai fini dell'applicazione del regime previsto dall'art. 9, par. 1, GDPR, non rileva che tali informazioni riguardino l'utente della piattaforma online o qualsiasi altra persona fisica per la quale l'ordine è stato effettuato [61]. In altre parole, alla luce delle implicazioni per i diritti e le libertà fondamentali degli interessati, i dati in questione devono essere considerati "dati relativi alla salute", anche qualora vi sia solo "una certa probabilità" che i medicinali ordinati siano destinati ai clienti della piattaforma [62].

L'interpretazione ampia adottata dalla Corte riguardo alla nozione di dati sensibili, inclusi quelli sanitari, rende praticamente impossibile limitare l'ambito di applicazione materiale del GDPR senza rischiare di pregiudicare la tutela offerta alle prerogative delle persone fisiche. Tuttavia, vi sono altre conseguenze da prendere in considerazione (v. *infra*), tra cui la difficoltà di delineare confini chiari rispetto ad altre normative che possono offrire una protezione uguale, se non più specifica e adeguata, agli individui [63]. In ambito sanitario, ad esempio, la direttiva 2011/24/UE e lo EHDS, pur rispettando la disciplina europea per i dati personali, perseguono obiettivi solo parzialmente

---

[60] Sentenza della Corte del 4 ottobre 2024, causa C-21/23, *Lindenapotheke*, ECLI:EU:C:2024:846, punto 84. Per un commento sulla pronuncia in questione, si rinvia a: A. FIORENTINI, *GDPR Meets Unfair Competition Law: The* Lindenapotheke *Ruling and Its Implications for Data Subjects and Controllers,* in *European Papers*, 2024, vol. 9, n. 3, pp. 852-864.

[61] *Ibid.* punti 86-88.

[62] *Ibid.* punto 90. Al contrario, l'Avvocato generale Szpunar, pur accogliendo l'interpretazione estensiva fornita dalla giurisprudenza della Corte sulla categoria dei dati sensibili, ritiene opportuno precisare il grado di certezza necessario per trarre conclusioni sullo stato di salute dell'interessato. Per evitare che la maggior parte dei trattamenti di dati relativi al commercio online rientri nel regime previsto dall'art. 9, par. 1, GDPR, l'Avvocato generale sottolinea la necessità di affinare l'interpretazione della nozione di "dati relativi alla salute" e, più in generale, di "dati sensibili". È essenziale, infatti, che le conclusioni derivanti dai dati relativi a un ordine online non siano mere supposizioni sullo stato di salute di chi effettua l'ordine. A tal fine, è fondamentale che il giudice del rinvio non consideri solo il contenuto dei dati, ma anche l'insieme delle circostanze relative al loro trattamento, inclusa l'identità del titolare del trattamento o il contesto in cui tale trattamento viene effettuato. Cfr. conclusioni dell'Avvocato generale Szpunar del 25 aprile 2024, causa C-21/23, *Lindenapotheke*, ECLI:EU:C:2024:354, punti 45-46 e 49.

[63] Ulteriori implicazioni verranno evidenziate nella sezione 3.2.

analoghi e adottano approcci regolatori non del tutto coincidenti. Basti pensare alle differenze tra il diritto di accesso ai dati personali sancito nel GDPR, che permette all'interessato di esercitare un controllo rispetto al trattamento avente ad oggetto i propri dati [64], il diritto alla cartella clinica previsto dalla direttiva 2011/24/UE, volto a garantire la continuità delle cure per i pazienti [65] e il diritto di accesso ai dati sanitari elettronici stabilito dallo EHDS [66], che si colloca a metà strada tra gli altri due.

2.2. I mezzi di conciliazione dei diritti e degli interessi in gioco

Il favore per la tutela della posizione degli interessati risulta evidente anche nei casi in cui la Corte si è pronunciata sull'interpretazione delle norme che sono state introdotte per gestire i possibili conflitti tra, da un lato, il legittimo interesse dei soggetti della vita economica e sociale degli Stati membri (ad es. le imprese e le amministrazioni nazionali) a disporre dei dati personali per svolgere le proprie attività nel mercato unico e, dall'altro, il diritto degli interessati alla protezione efficace di questi dati [67]. Per mitigare il rischio di tali conflitti, sia la DPD sia il successivo GDPR prevedono specifici meccanismi di conciliazione, inseriti nel testo normativo sottoforma di disposizioni che consentono di bilanciare la tutela dei diritti e delle libertà degli individui riguardo ai dati personali con gli interessi del titolare [68] e, ove rilevante, l'interesse pubblico [69].

---

[64] Art. 15 GDPR.

[65] Art. 4, par. 2, lett. f), direttiva 2011/24/UE.

[66] Art. 3 EHDS.

[67] Parafrasi del testo della sentenza *Lindqvist*, punti 79-81.

[68] Tra queste, si possono ricordare: l'art. 6, par. 1, lett. f), GDPR che permette al titolare di provare l'esistenza di un "legittimo interesse" su cui fondare il proprio trattamento; il test di compatibilità tra il trattamento primario e quello ulteriore che, se superato, consente di non dover trovare una base giuridica per il trattamento ulteriore diversa da quella del trattamento originario (art. 6, par. 4, GDPR); le condizioni da soddisfare per poter trattare categorie speciali di dati (art. 9, par. 2, GDPR); le deroghe ai diritti degli interessati in generale (art. 23 GDPR) e in caso di trattamento ai fini di ricerca scientifica (art. 89, parr. 2 e 3, GDPR); i limiti posti al campo di applicazione del diritto alla portabilità (art. 20 GDPR); le condizioni per poter eseguire trattamenti automatizzati (art. 22 GDPR); la possibilità di effettuare una valutazione d'impatto e adottare misure tecniche e organizzative, nonché codici di condotta e meccanismi di certificazione per dimostrare la propria conformità alla disciplina (artt. 35, 40 e 42 GDPR).

[69] Il capo IX del GDPR consente il bilanciamento tra il diritto alla protezione dei dati personali e, *inter alia*, la libertà di espressione e d'informazione (art. 85), il diritto d'accesso ai documenti (art. 86), la libertà delle arti e delle scienze e il diritto alla salute (art. 89), la libertà di pensiero, di coscienza e religione (art. 91). In particolare, a questo proposito sono

A titolo esemplificativo, tra le norme che dovrebbero permettere questo tipo di bilanciamento vi sono quelle concernenti il diritto dell'interessato ad accedere ai propri dati personali [70] e quelle relative al trattamento di "categorie particolari di dati personali", tra cui quelli sanitari. Per quanto riguarda il diritto all'accesso ai dati, che include anche il diritto a ottenere una copia dei dati oggetto di trattamento [71], possono essere previste limitazioni specifiche per salvaguardare altri interessi. Con riferimento, invece, ai dati sensibili, vediamo che il divieto generale di trattare questa categoria di dati può essere derogato in determinate circostanze, come l'ottenimento del consenso esplicito da parte dell'interessato o la sussistenza di un interesse pubblico rilevante.

La scelta di concentrarsi sulla giurisprudenza della Corte relativa alla portata del diritto di accesso ai dati personali (sezione 2.2.1) e alle norme concernenti il trattamento dei dati sensibili (sezione 2.2.2) è motivata dall'importanza che tali disposizioni assumono anche nell'ambito dello EHDS. Questo strumento normativo, infatti, prevede un diritto (non assoluto) di accesso ai dati sanitari elettronici e stabilisce regole specifiche per l'uso primario e secondario di dati sensibili, ossia quelli sanitari elettronici personali. Pertanto, l'analisi che svolgeremo in questa sezione è funzionale alle considerazioni che verranno sviluppate in quella successiva.

2.2.1. Il diritto di accesso ai dati personali e le possibili limitazioni

Il diritto di accesso ai dati personali occupa una posizione di rilievo nella disciplina europea sui dati personali. In primo luogo, è l'unico diritto, insieme a quello di rettifica, a essere menzionato all'interno dell'art. 8, par. 2, Carta.

---

emblematiche le regole sul trattamento dei dati per finalità giornalistiche (artt. 17 e 85, e considerando 154 GDPR). Si vedano, inoltre, la sentenza *Google LLC c. CNIL*, punto 61 e la sentenza del 24 settembre 2019, causa C-136/17, *GC e a. c. CNIL*, ECLI:EU:C:2019:773, punto 59, dove la Corte riconosce che l'art. 17, par. 3, lett. a), GDPR rappresenta il tentativo del legislatore di bilanciare il diritto alla protezione dei dati con la libertà d'informazione.

[70] Un ulteriore esempio è rappresentato dal diritto alla deindicizzazione di cui all'art. 12, lett. b), DPD e art. 17 GDPR, sulla cui portata si è espressa la Corte nella sentenza *Google Spain*, e nelle sentenze del 24 settembre 2019, causa C-507/17*, Google LLC c. CNIL*, ECLI:EU:C:2019:772 e dell'8 dicembre 2022, causa C-460/20, *Google (Ricerca di contenuti presumibilmente inesatti)*, ECLI:EU:C:2022:962. Tra le altre cose, in queste occasioni, i giudici hanno chiarito alcuni criteri che i gestori del motore di ricerca, a cui viene presentata la richiesta di deindicizzazione, e le autorità nazionali devono utilizzare per bilanciare i diritti dell'interessato con l'interesse economico del titolare e l'interesse del pubblico ad accedere all'informazione.

[71] Linee guida dell'EDPB n. 01/2022 sui diritti dell'interessato – diritto di accesso ai dati, versione 2.1, p. 14, in cui si afferma che "[l]'obbligo di fornire una copia non dev'essere inteso come un ulteriore diritto dell'interessato, ma come una modalità di concessione dell'accesso ai dati".

In secondo luogo, il diritto all'accesso ai dati svolge un ruolo strumentale e funzionale rispetto all'esercizio di altre prerogative dell'interessato, tra cui il diritto di rettifica, di cancellazione e limitazione del trattamento [72]. Tale diritto include la possibilità per l'interessato di ottenere informazioni relative al trattamento dei propri dati, i dati oggetto di tale trattamento e i destinatari a cui tali dati sono stati comunicati [73], nonché una prima copia gratuita dei dati processati [74].

In ragione della natura non assoluta del diritto alla protezione dei dati personali [75] e quindi anche del diritto di accesso a tali dati, sono previste alcune limitazioni. Nel vigore della DPD, il responsabile (oggi, titolare) del trattamento non doveva comunicare all'interessato i destinatari dei dati oggetto di trattamento, nel caso in cui ciò risultasse impossibile o implicasse uno sforzo proporzionato [76], oppure qualora una restrizione fosse necessaria per la salvaguardia, *inter alia*, di diritti e libertà altrui [77]. Oltre a queste ipotesi, confermate dagli artt. 15, par. 4 e 23, par. 1, lett. i), GDPR, il regolamento stabilisce che il diritto di accesso ai dati può essere limitato quando: i) le richieste

---

[72] Sentenza della Corte del 27 febbraio 2025, causa C-203/22, *CK*, ECLI:EU:C:2025:117, punto 54; sentenze *Pankki S*, punto 58 e *Osterreichische Datenschutzbehörde e CRIF*, punto 35; sentenze del 20 dicembre 2017, causa C-434/16, *Nowak*, EU:C:2017:994, punto 57; del 17 luglio 2014, causa C-141/12 e C-372/12, *YS e Minister voor Immigratie, Integratie en Asiel*, EU:C:2014:2081, punto 44; del 7 maggio 2009, causa C-553/07, *Rijkeboer*, ECLI:EU:C:2009:25, punti 51-52.

[73] Art. 12 DPD e art. 15 GDPR.

[74] Art. 15, par. 3, GDPR. Per un commento sul diritto di accesso, cfr. EDPB, *Guidelines on the Right of Access and Letter in Cookie Consent*, 2022. In dottrina, v. L. NAUDTS, P. DEWITTE, J. AUSLOOS, *Meaningful Transparency through Data Rights: A Multidimensional Analysis*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022, p. 546 ss.; G. ZANFIR-FORTUNA, *Article 15. Right of Access by the Data Subject*, in C. KUNER et al. (eds.), *The EU General Data Protection Regulation – A Commentary*, OUP, Oxford, 2020, p. 462; J. AUSLOOS, R. MAHIEU, M. VEALE, *Getting Data Subject Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance*, in *JIPITEC*, 2020, vol. 10, p. 293.

[75] Cfr., *inter alia*, sentenza della Corte del 21 dicembre 2023, causa C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:1022, punto 54; sentenza *Google (Ricerca di contenuti presumibilmente inesatti)*, punto 56; sentenza del 16 luglio 2020, causa C-311/18, *Schrems II*, ECLI:EU:C:2020:559, punto 92; sentenze *GC e a. c. CNIL*, punto 58, *Google LLC c. CNIL*, punto 60; parere della Corte n. 1/15 del 26 luglio 2017, ECLI:EU:C:2017:592, punto 136; sentenze del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970, punti 96 e 103, dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, punto 52, del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, C-92/09 e C-93/09, EU:C:2010:662, punto 48; sentenza *Satakunnan Markkinapörssi e Satamedia*, punto 56.

[76] Art. 12, lett. c), DPD.

[77] Art. 13, par. 1, lett. g), DPD.

dell'interessato sono manifestamente infondate ed eccessive [78] e ii) l'interessato ha presentato più richieste di copie dei dati oggetto di trattamento [79].

La Corte è stata chiamata più volte a pronunciarsi sul diritto di accesso ai dati personali e, in particolare, sulla legittimità di norme nazionali che ne limitano la portata in modi e per finalità differenti. Un primo esempio è rappresentato dalla causa *Rijkeboer*, concernente il rapporto tra l'obbligo del titolare di cancellare i dati quando non sono più necessari per le finalità per cui sono stati raccolti o successivamente trattati [80] e il diritto di accesso dell'interessato [81]. In questa occasione, la Corte ha stabilito che la legge olandese, imponendo un limite di un anno all'obbligo di conservazione dei dati, non costituisce "un giusto equilibrio tra, da una parte, l'interesse della persona interessata a tutelare la propria vita privata, in particolare per mezzo dei diritti alla rettifica, alla cancellazione ed al congelamento dei dati, in caso di non conformità del loro trattamento con la direttiva, nonché del diritto di opposizione e del diritto ad agire in giudizio, e, dall'altra, l'onere che l'obbligo di conservare tali informazioni comporta per il responsabile del trattamento" [82]. Tuttavia, i giudici hanno anche osservato che una limitazione temporale simile può essere considerata proporzionata se si dimostra che la conservazione dei dati per un periodo di tempo maggiore comporterebbe un onere eccessivo per il titolare del trattamento [83].

Nel pervenire alla sua conclusione, dunque, la Corte sembra orientare il "giusto equilibrio" di cui sopra a favore di una maggiore attenzione verso la

---

[78] Secondo l'art. 12, par. 5, GDPR, dopo aver dimostrato il carattere manifestamente infondato della richiesta, il titolare del trattamento può decidere di: i) addebitare un contributo spese ragionevole; o ii) rifiutare la richiesta.

[79] Art. 15, par. 3, GDPR. In queste ipotesi, il titolare del trattamento può addebitare un contributo spese ragionevole. Inoltre, il quarto paragrafo della medesima disposizione afferma che il diritto di ottenere una copia "non deve ledere i diritti e le libertà altrui".

[80] Art. 6, par. 1, lett. e), DPD.

[81] Art. 12, par. 1, lett. l), DPD.

[82] Sentenza *Rijkeboer*, punto 64. Tale causa riguarda la richiesta del sig. Rijkeboer alla giunta comunale di Rotterdam di ottenere un elenco delle comunicazioni a terzi dei suoi dati personali (ad es. il suo nome, l'indirizzo, i destinatari e le categorie di destinatari) avvenute nei due anni precedenti la sua domanda. La giunta comunale però ha respinto la richiesta, fornendo solo i dati relativi all'anno precedente, in conformità alla legge olandese sulla gestione dei dati personali da parte dei comuni, che recepisce la DPD e che limita l'obbligo di comunicare all'interessato i dati trasmessi a terzi nel corso dell'anno precedente la richiesta. Il sig. Rikeboer ha impugnato la decisione della giunta comunale presso il tribunale amministrativo e successivamente presso il tribunale di Rotterdam, che ha annullato la decisione della giunta. Quest'ultima ha interposto appello alla sezione per il contenzioso amministrativo, che ha sottoposto la questione alla Corte in via pregiudiziale.

[83] *Ibid.* punto 66.

tutela della posizione del titolare del trattamento [84]. Diversamente, l'Avvocato generale Ruiz-Jarabo Colomer, pur giungendo al medesimo risultato, ha enfatizzato il carattere "garantista" e la "vocazione" soggettiva della DPD per sottolineare il "valore preminente" che questa normativa attribuisce alla tutela dell'interessato [85]. Pertanto, nel ritenere che gli artt. 6 e 12 DPD ostavano a una normativa nazionale che limitava l'obbligo di conservazione a un solo anno, l'Avvocato generale ha riconosciuto che una tale restrizione può essere considerata proporzionata non tanto se si dimostra che il rispetto di questo obbligo risulta essere eccessivamente oneroso per il titolare, ma piuttosto se viene garantito all'interessato un adeguato livello di informazioni che gli permetta di esercitare il proprio diritto di accesso senza restrizioni [86].

L'approccio interpretativo dell'Avvocato generale Ruiz-Jarabo Colomer appena riportato, che pone al centro la tutela dell'interessato, è destinato a trovare accoglimento nella giurisprudenza successiva, la quale – come riferito – può contare sulle novità introdotte nel quadro costituzionale dall'entrata in vigore del Trattato di Lisbona. Questa giurisprudenza interpreta le norme europee sui dati personali ponendo il diritto individuale alla protezione dei dati personali, nelle sue varie manifestazioni (ad es. diritto di accesso e di cancellazione), come prioritario rispetto ad altri diritti e interessi coinvolti nei casi di trattamento dei dati personali.

Emblematica, a questo proposito, è la causa *FT*, che riguarda l'interpretazione del diritto di accesso alla copia dei dati sanitari contenuti nella cartella clinica dell'interessato. In questo caso, il limite posto al diritto di accesso ai dati, e in particolare alla richiesta di ottenere una copia degli stessi (più precisamente, dell'intera cartella clinica) [87], è rappresentato dalla possibilità prevista dalla normativa tedesca per i medici di rifiutarsi di mettere a disposizione gratuitamente la documentazione clinica richiesta dal paziente.

Per prima cosa, la Corte ha chiarito che il diritto di accedere ai dati relativi alla salute e il diritto di ottenere una prima copia a titolo gratuito non possono essere limitati – né tramite un diniego di accesso né mediante la richiesta di pagamento di un corrispettivo – a uno dei motivi elencati nel considerando

---

[84] *Ibid.* punto 60.

[85] Conclusioni dell'Avvocato generale Ruiz-Jarabo Colomer del 22 dicembre 2008, causa C-212/13, *Ryneš*, ECLI:EU:C:2008:773, punto 70.

[86] *Ibid.* punto 71.

[87] A questo proposito, è stato sottolineato che, nel caso specifico, sarebbe stato più corretto invocare non tanto il diritto di accesso previsto nel GDPR, bensì il diritto alla cartella medica stabilito dal codice civile tedesco (v. *infra* nota 97) e, in situazioni transfrontaliere, dalla direttiva 2011/24/UE. Cfr. G. DI FEDERICO, *From Dusk Till Dawn. The Case of F.T. v D.W. and the Right to Access Electronic Medical Records in Light of the Future European Health Data Space Regulation*, in *European papers*, 2024, vol. 9, n. 2, pp. 463-477.

63, prima frase, GDPR [88]. In altre parole, come già affermato dall'EDPB nelle sue linee guida sull'accesso ai dati personali [89], la richiesta non può essere respinta se con essa si persegue un motivo diverso da quello di essere consapevole del trattamento dei dati e di verificarne la liceità [90]. Secondo la Corte, il non dover giustificare la richiesta di accesso ai dati contribuisce "necessariamente" ad agevolare l'esercizio dei diritti previsti dal GDPR, realizzando così gli obiettivi precipui di questa normativa: assicurare un livello coerente ed elevato di protezione delle persone fisiche all'interno dell'Unione, nonché rafforzare e disciplinare dettagliatamente i diritti degli interessati [91].

L'esercizio di questo diritto, quindi, viene svincolato dalla *ratio* che ne ha giustificato l'inserimento nel GDPR e che lo rende strumentalmente connesso agli altri diritti, come il diritto di rettifica e di opposizione [92]. Il fatto che il paziente possa invocare qualsiasi motivo per giustificare una richiesta di accesso potrebbe portare a un incremento significativo nel suo utilizzo, anche per finalità lesive di interessi giuridici altrui [93]. Nel caso di specie, ad esempio,

---

[88] Sentenza della Corte del 26 ottobre 2023, causa C-307/22, *FT (Copie di cartelle cliniche)*, ECLI:EU:C:2023:811, punto 46. Il rinvio pregiudiziale in oggetto prende le mosse da una controversia sorta tra un paziente DW che ha ricevuto cure dentistiche da FT, dopo che quest'ultimo ha richiesto a DW di farsi carico delle spese sostenute per la fornitura della copia della sua cartella medica.

[89] Linee guida dell'EDPB n. 01/2022 sui diritti degli interessati in cui si afferma che "*data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met, the purposes behind the request should be regarded as irrelevant*".

[90] Sentenza *FT (Copie di cartelle cliniche)*, punto 43.

[91] *Ibid.* punti 47 e 50.

[92] In particolare, la dottrina riconosce come principale obiettivo del diritto di accesso quello di migliorare la trasparenza e facilitare il controllo degli interessati. Cfr., *inter alia*, G. ZANFIR-FORTUNA, *op. cit.*, 2020, p. 452 e H. KRANENBORG, *Article 8 – Protection of Personal Data*, in S. PEERS et al. (eds.), *The EU Charter of Fundamental Rights, A Commentary*, Hart Publishing, Oxford, 2021, p. 272. In giurisprudenza, sul rapporto di strumentalità del diritto di accesso rispetto all'esercizio degli altri diritti che il GDPR attribuisce agli interessati, cfr. sentenze *Pankki S*, punto 58 e *Osterreichische Datenschutzbehörde e CRIF*, punto 35; sentenza del 12 gennaio 2023, causa C-154/21, *RW c. Österreichische Post AG*, ECLI:EU:C:2023:3, punto 38. Lo stesso era stato stabilito con riferimento alla DPD nelle sentenze *Nowak*, punto 57; *YS e Minister voor Immigratie, Integratie en Asiel*, punto 44 e *Rijkeboer*, punti 51 e 52.

[93] Non è forse un caso che la Commissione, nel *Digital Omnibus*, proponga – tra le varie modifiche al GDPR – la possibilità, qualora l'interessato abusi del diritto di accesso per finalità estranee alla protezione dei dati, che il titolare del trattamento possa: i) richiedere un contributo spese ragionevole, tenuto conto dei costi amministrativi sostenuti per fornire le informazioni, la comunicazione o per adottare l'azione richiesta; oppure ii) rifiutare di dare seguito alla richiesta (art. 3, par. 4, proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 e delle 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)

l'interessato ha manifestato l'intenzione di voler accedere a tali dati per verificare se sussistono motivi per richiedere un risarcimento in materia di responsabilità medica, sospettando la mancanza di correttezza nelle cure dentistiche ricevute. Inoltre, l'affermazione secondo cui i motivi addotti per giustificare la richiesta di accesso ai dati sono irrilevanti potrebbe mettere in dubbio la legittimità di norme nazionali che invece impongono al richiedente di rendere note le ragioni alla base della propria domanda [94].

Oltre a non poter essere circoscritto sulla base dei motivi che giustificano la necessità di conoscere i dati trattati, la Corte, allineandosi all'interpretazione fornita dall'EDPB [95], ha confermato il principio di gratuità della prima copia dei dati, secondo il quale il diritto di accesso ai dati non può essere soggetto a restrizioni da parte di normative nazionali che consentono al titolare del trattamento di addebitare all'interessato che ha esercitato tale diritto i costi relativi alla fornitura della prima copia dei dati. Questo perché, sebbene il diritto di accesso non sia assoluto [96], la normativa nazionale in questione "porta a scoraggiare non soltanto le richieste inutili, ma anche le richieste dirette ad ottenere per un motivo legittimo una prima copia, a titolo gratuito, dei dati personali trattati [97]. Di conseguenza, essa viola necessariamente il principio di gratuità della prima copia e rimette quindi in discussione l'effetto utile del diritto di accesso" [98].

2018/1807, (UE) 2019/1150, (UE) 2022/868 e della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025).

[94] Ad esempio, il Codice privacy italiano prevede che nel caso di richiesta di accesso a documenti contenenti dati idonei a rivelare lo stato di salute e la vita sessuale, questa deve essere motivata dalla documentata necessità di esercitare o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, o un diritto della personalità o altro diritto e libertà fondamentale o di tutelare una situazione giuridicamente rilevante di rango pari a quella dell'interessato, o un diritto della personalità o altro diritto o libertà fondamentale (art. 60, d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018).

[95] Linee guida dell'EDPB n. 01/2022, p. 13, in cui si afferma che "*[t]he controller must ensure that the first copy is free of charge, even where it considers the cost of reproduction to be high (example: the cost of providing a copy of the recording of a telephone conversation)*".

[96] Sentenza *FT (Copie di cartelle cliniche)*, punto 62.

[97] In particolare, il codice civile tedesco stabilisce che il professionista sanitario è obbligato a tenere, a fini di documentazione, una cartella medica in forma cartacea o elettronica, in cui registrare tutte le misure essenziali dal punto di vista medico per il trattamento in corso e futuro, nonché i relativi risultati (ad es. l'anamnesi, le diagnosi, gli esami, i risultati di esami) (art. 630f). Oltre a tale obbligo per il professionista, il diritto tedesco riconosce al paziente il diritto di accedere immediatamente all'intera cartella medica che lo riguarda (non ai soli dati personali), salvo che motivi terapeutici importanti o altri diritti rilevanti di terzi impediscano la consultazione. Il paziente ha anche diritto di ottenere copie elettroniche della cartella medica, rimborsando al professionista sanitario i costi sostenuti.

[98] Sentenza *FT (Copie di cartelle cliniche)*, punto 65.

La Corte ha anche escluso che la fattispecie in esame possa rientrare nelle eccezioni previste dall'art. 15, par. 4, GDPR, secondo cui "il diritto di ottenere una copia […] non deve ledere i diritti e le libertà altrui", o dall'art. 23, par. 1, lett. i), GDPR, per cui una limitazione del diritto di accesso è possibile "qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare […] la tutela […] dei diritti e delle libertà altrui" [99]. Tuttavia, nel giungere a questa conclusione, i giudici non hanno esaminato in modo dettagliato il mancato rispetto di tali condizioni, limitandosi a dichiarare che gli obiettivi di tutela degli interessi economici dei professionisti sanitari previsti dalla legge tedesca non possono essere considerati "diritti e libertà altrui" ai sensi dell'art. 23, par. 1, lett. i), GDPR.

Questo tipo di interpretazioni, incentrate sulla tutela dei diritti degli interessati, corre il rischio di sacrificare indebitamente gli interessi dei titolari del trattamento che la stessa disciplina consentirebbe di valorizzare. In particolare, le interpretazioni che riconoscono quasi automaticamente la prevalenza del diritto degli interessati alla protezione dei dati personali potrebbero compromettere la realizzazione dei molteplici obiettivi che la disciplina europea sui dati persegue. Come vedremo in seguito, tale normativa non è stata concepita solo per garantire agli interessati un elevato livello di tutela, ma anche per consentire a soggetti terzi, portatori di interessi propri o della collettività, di trarre beneficio dal potenziale economico e sociale dei dati personali [100].

2.2.2. I dati sensibili e le deroghe al divieto generale di trattamento

Nella disciplina europea per i dati personali, i dati sensibili, tra cui quelli relativi alla salute, sono soggetti a un regime di tutela speciale [101]. Già con la direttiva madre, il loro trattamento è stato, in linea di principio, vietato. Questo divieto generale ha lo scopo di assicurare una "maggiore protezione" contro trattamenti che, avendo come oggetto dati particolarmente sensibili, possono determinare un'ingerenza grave nei diritti di cui agli artt. 7 e 8 della Carta [102]. Si pensi, ad esempio, alle conseguenze discriminatorie e di stigmatizzazione

[99] *Ibid.* punti 60-61.

[100] Si veda, in particolare, la sezione 3.2 del presente capitolo.

[101] Art. 8 DPD e art. 9 GDPR. Rispetto alla direttiva madre, il GDPR ha ampliato l'elenco di tipologie di dati personali sensibili, così come le ipotesi derogatorie al divieto generale di trattamento.

[102] Sentenze *Krankenversicherung Nordrhein*, punto 40, *Commissione europea c. Repubblica di Polonia*, punto 345 e *Vyriausioji tarnybinės etikos komisija*, punti 125-126; sentenza del 6 ottobre 2020, causa C-623/17, *Privacy International*, ECLI:EU:C:2020:790, punto 71 e sentenza *GC e a. c. CNIL*, punto 44.

che potrebbero derivare dall'utilizzo improprio dei dati relativi alla salute. I casi di scuola, al riguardo, concernono l'utilizzo di dati sanitari da parte dei datori di lavoro per decidere se assumere o meno una persona che risulta avere un elevato rischio di sviluppare una certa patologia [103] oppure da parte delle compagnie assicurative per fissare un premio maggiore sulla base di misurazioni ripetute della pressione arteriosa lungo un certo arco di tempo che fanno presumere che il soggetto in questione sia esposto a un rischio più elevato di attacchi cardiaci [104].

A fronte dei rischi associati al trattamento di categorie particolari di dati, il legislatore europeo ha previsto, oltre al divieto generale di cui sopra, una serie di garanzie aggiuntive che contribuiscono a offrire una tutela rafforzata qualora tali dati vengano trattati (ad es. lo svolgimento della valutazione d'impatto in caso di trattamenti su larga scala e l'obbligo di designazione del responsabile della protezione dei dati personali) [105].

Al tempo stesso, è stata ammessa una serie di ipotesi in cui, sulla base di specifiche condizioni di liceità, i dati sensibili possono essere trattati [106]. Questa scelta permette, in ambito sanitario, di preservare il valore dei dati relativi alla salute per le persone fisiche e per l'intera collettività [107]. In particolare, favorisce lo sviluppo della medicina "predittiva, preventiva, partecipativa e personalizzata" [108], che consente di intervenire in modo celere durante la fase precoce della malattia e di definire percorsi terapeutici su misura grazie alla possibilità di disporre di grandi quantità di dati non solo sulla storia clinica del paziente, ma anche provenienti in tempo reale dalla c.d. *Medical Internet of Things* [109].

---

[103] S. BAROCAS, A.D. SELBST, *Big Data's Disparate Impact*, in *Cal. Law Rev.*, 2016, vol. 104, pp. 671-732; E.D. DE ARMOND, *To Cloack the Within: Protecting the Employees from Personality Testing*, in *DePaul Law Rev.*, 2012, vol. 61, pp. 1136-1137.

[104] EDPS, *Opinion on the Communication from the Commission eHealth Action Plan 2012-2020-Innovative Healthcare for the 21st Century*, 2013, p. 6; K.B. BROTHERS, M.A. ROTHSTEIN, *Ethical, Legal and Social Implications of Incorporating Personalized Medicine into Healthcare*, in *Future Med.*, 2014, vol. 15, pp. 43-51. In generale, sulle discriminazioni legate all'uso dei dati genetici in ambito lavorativo e assicurativo, cfr. P.M. SCHWARTZ, *Privacy and the Economics of Personal Health Care Information*, in *Tex. L. Rev.*, 1997, vol. 76, n. 2, pp. 28-30.

[105] Artt. 35, par. 3, lett. b) e 37, par. 1, lett. c), GDPR.

[106] Art. 8, par. 2, DPD e art. 9, par. 2, GDPR.

[107] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati, COM(2020) 66 final, p. 2.

[108] M. BOCCI, *Veronesi e le quattro "p" della nuova medicina*, in *La Repubblica Firenze.it*, 2013 (https://firenze.repubblica.it/cronaca/2013/06/07/news/veronesi-60592718).

[109] Termine con cui si intende l'insieme di strumenti tecnologici di ultima generazione, quali *smartphone* e *smartwatch* che si avvalgono di una molteplicità di sensori capaci di

Nonostante gli spazi concessi dal legislatore europeo per utilizzare e condividere i dati sanitari per finalità di interesse generale, la giurisprudenza della Corte ha interpretato in modo restrittivo le ipotesi di trattamento dei dati sensibili, facendo leva sulla loro natura derogatoria [110]. Limitando eccessivamente la portata delle condizioni previste all'art. 9, par. 2, GDPR, specialmente quelle che consentono un bilanciamento dei diritti e degli interessi in gioco [111], il rischio è di ridurre le possibilità di effettuare trattamenti di dati sensibili a causa della difficoltà per il titolare di provare l'esistenza di una base giuridica valida.

L'eventualità che tale rischio si verifichi aumenta se si considera l'affermarsi di un orientamento interpretativo secondo il quale, in caso di trattamento dei dati sensibili, il titolare del trattamento dovrebbe dimostrare il rispetto di una delle condizioni di liceità non solo tra quelle dell'art. 9, par. 2, GDPR, ma anche tra quelle contemplate dall'art. 6, par. 1, GDPR [112]. Quest'ultima disposizione stabilisce un elenco esaustivo e tassativo di situazioni in cui un trattamento di dati "comuni", ossia non sensibili, può essere considerato lecito [113]: ad esempio, lo è nel caso in cui l'interessato ha espresso il suo consenso [114] oppure se l'attività di trattamento è necessaria per l'esecuzione di un contratto di cui l'interessato è parte [115], per l'adempimento di un

---

rilevare segnali vitali come il battito cardiaco, la pressione sanguigna e i livelli di glucosio nel sangue. Cfr. H. FARHADI, *Medical Internet of Things (m-IoT): Enabling Technologies and Emerging Applications*, in *IntechOpen*, 2019 e Z. AHMED et al., *Artificial Intelligence with multi-factual machine learning platform development for better healthcare and precision medicine*, in *Database*, 2020, p. 1.

[110] Da ultimo, v. la sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms e a*., ECLI:EU:C:2023:537, punto 76. Come vedremo in seguito, l'affermazione relativa al secondo paragrafo dell'art. 9 GDPR è stata recentemente temperata dalla stessa Corte, la quale ha affermato che il divieto di cui all'art. 9, par. 1, GDPR "non può determinare una riduzione dell'ambito di applicazione di un'altra disposizione di tale regolamento contraria al chiaro tenore letterario di quest'ultima" (sentenza *Krankenversicherung Nordrhein*, punto 51).

[111] Cfr. art. 9, par. 2, lett. g)-j), GDPR.

[112] Parere del WP n. 06/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE.

[113] Per un approfondimento sul tema, v. L. CALIFANO et al., *La protezione dei dati personali, natura, garanzie e bilanciamento di un diritto fondamentale*, Giappichelli, Torino, 2023, p. 193 ss.

[114] Art. 6, par. 1, lett. a), GDPR. Le caratteristiche del consenso sono poi specificate all'art. 4, par. 11, GDPR ("manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato") e dalla Corte (ad es. sentenze dell'11 novembre 2022, causa C-61/19, *Orange Romania*, ECLI:EU:C:2020:901 e del 1° ottobre 2019, causa C-673/17, *Planet 49*, ECLI:EU:C:2019:801).

[115] Art. 6, par. 1, lett. b), GDPR.

obbligo legale o l'esecuzione di un compito di interesse pubblico [116], nonché per la salvaguardia degli interessi vitali dell'interessato [117] e per il perseguimento del legittimo interesse del titolare del trattamento o di terzi [118].

La soluzione interpretativa di cumulare le due disposizioni può risultare problematica se si considera che le condizioni di liceità in esse previste non coincidono perfettamente [119]. Pertanto, il titolare che effettua un trattamento di dati sensibili deve necessariamente conformarsi sia all'art. 9, par. 2, GDPR sia all'art. 6, par. 1, GDPR. Questo significa, ad esempio, che, anche se dimostrasse l'esistenza di una base giuridica diversa dal consenso esplicito ai sensi dell'art. 9, par. 2, lett. a), GDPR – requisito che, come vedremo, risulta particolarmente difficile da soddisfare –, il titolare dovrebbe comunque provare che il suo trattamento si basa su uno dei presupposti di liceità stabiliti dall'art. 6, par. 1, GDPR, tra cui il consenso che ha assunto un ruolo preminente [120].

Nonostante la normativa europea sui dati personali non dia un ordine prioritario alle giustificazioni al trattamento [121], infatti, i giudici di Lussemburgo hanno affermato che le condizioni di cui all'art. 6, par. 1, lett. b)-f), GDPR devono essere interpretate restrittivamente, dal momento che rendono lecito un trattamento effettuato in assenza di consenso [122]. In questo modo, la posizione

---

[116] Art. 6, par. 1, lett. c) e e), GDPR. In entrambi i casi, l'obbligo legale del titolare e il compito di interesse pubblico di cui è investito devono essere previsti dal diritto dell'Unione o dal diritto nazionale a cui è soggetto il titolare (art. 6, par. 3, GDPR).

[117] Art. 6, par. 1, lett. d), GDPR.

[118] Art. 6, par. 1, lett. f), GDPR.

[119] Se alcune lettere dell'art. 9, par. 2, GDPR assorbono quelle dell'art. 6 GDPR (ad es. lett. a), c), g) e i)), altre invece no (ad es. lett. e) e h)). Sul punto, si rinvia alle osservazioni dell'Avvocato generale Campos Sánchez Bordona del 25 maggio 2023, causa C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:433, punto 61.

[120] A tale proposito, è bene precisare che il consenso potrebbe essere richiesto non tanto come consenso *ex* art. 6, par. 1, GDPR, ma come garanzia – prevista a livello nazionale – per il trattamento di dati sensibili *ex* art. 9, par. 4, GDPR.

[121] Secondo l'art. 6, par. 1, un "trattamento è lecito solo se e nella misura in cui ricorre *almeno una* delle […] condizioni" di liceità elencate (corsivo aggiunto). Così anche l'art. 8, par. 2, Carta, che non prevede differenze tra il consenso e "ogni altro fondamento legittimo previsto dalla legge".

[122] Sentenza del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, ECLI:EU:C:2024:857, punto 31 e sentenza *Meta Platforms e a*., punto 93. A tale proposito è importante sottolineare che la giurisprudenza citata a sostegno di questa conclusione afferma un principio parzialmente differente, ossia che le limitazioni e le esenzioni alla tutela e alla protezione dei dati personali devono essere interpretate nei limiti dello stretto necessario. Questo comporta, ad esempio, che il titolare, quando agisce per un interesse pubblico *ex* art. 6, par. 1, lett. e), GDPR, deve rispettare il principio di "minimizzazione dei dati" di cui all'art. 5, par. 1, lett. c), GDPR (sentenza *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punto 73), e deve verificare che tale obiettivo non può essere raggiunto con mezzi

del titolare del trattamento risulta aggravata, poiché è tenuto a ottenere il consenso di default qualora non riesca a dimostrare l'esistenza di una delle altre basi giuridiche dell'art. 6, par. 1, GDPR, di cui, in ogni caso, la Corte ha fornito una lettura rigorosa e restrittiva [123]. Ad esempio, per quanto riguarda la necessità di salvaguardare un interesse vitale dell'interessato di cui all'art. 6, par. 1, lett. d), GDPR, una base giuridica che ha un corrispettivo diretto nell'art. 9, par. 2, lett. c), GDPR, la Corte ha confermato la sua natura residuale. Tale condizione di liceità dovrebbe ritenersi adeguata solo nelle situazioni in cui è in gioco la vita dell'interessato e dovrebbe presumersi esclusa qualora l'attività del titolare abbia un carattere essenzialmente economico e commerciale [124].

Inoltre, con riferimento ai presupposti di liceità che richiedono di effettuare un bilanciamento, come l'art. 6, par. 1, lett. e) e f), GDPR, e che possono essere rilevanti anche per giustificare il trattamento di dati sanitari, la Corte tende a conferire alla tutela del diritto individuale alla protezione dei dati personali un peso significativamente maggiore rispetto ad altri diritti e interessi. Se in alcuni casi tale approccio appare meno problematico, poiché la conclusione raggiunta deriva da un'attenta valutazione del soddisfacimento di requisiti di bilanciamento specifici [125], maggiormente controversi sono quei casi in cui la prevalenza del diritto fondamentale alla protezione dei dati personali sembra derivare da un automatismo, connesso alla centralità che questo diritto ricopre nell'interpretazione delle norme del GDPR.

In *Endemol Shine*, ad esempio, la Corte ha concluso che l'obbligo di comunicare i dati relativi a condanne penali, imposto da una legge nazionale (finlandese) a un organo giurisdizionale per garantire l'accesso del pubblico a

---

meno pregiudizievoli per i diritti fondamentali degli interessati (sentenza *Latvijas Republikas Saeima (Punti di penalità)*, punto 110). Lo stesso vale per i trattamenti che si fondano su un interesse legittimo del titolare (sentenze dell'11 dicembre 2019, causa C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064, punti 46 e 47 e del 4 maggio 2017, causa C-13/16, *Rīgas satiksme*, EU:C:2017:336, punto 30).

[123] Tale approccio si colloca nel solco delle interpretazioni fornite dal WP relativamente alla DPD. Cfr. parere del WP n. 06/2014, p. 24.

[124] Sentenza *Meta Platforms e a.*, punto 137. Nel parere del WP n. 06/2014, il WP evidenzia come, in ragione dell'ampiezza della formulazione della disposizione in questione (ad es. non specifica se la minaccia all'interesse essenziale alla vita della persona interessata deve essere immediata), sia necessario attribuire a questa condizione di liceità un'applicazione di portata limitata. L'interesse vitale dovrebbe riguardare unicamente i casi di vita o di morte, o almeno di una minaccia grave alla salute dell'interessato o di un terzo. Inoltre, il WP sottolinea che tale base giuridica non è adeguata a "legittimare la raccolta e il trattamento di un'ingente quantità di dati personali" (p. 24), dovendosi preferire – ogniqualvolta sia possibile – il ricorso al consenso.

[125] Sentenze *Commissione europea c. Repubblica di Polonia (Indipendenza e privacy dei giudici)*, punto 340 e *Vyriausioji tarnybinės etikos komisija*, punti 83-113 con riferimento, rispettivamente, agli art. 6, par. 1, lett. c) e e) e 9, par. 2, lett. g), GDPR, nonché sentenza *Meta Platforms e a.*, punti 108-112 per quanto riguarda l'art. 6, par. 1, lett. f), GDPR.

documenti ufficiali, non può fondarsi sugli artt. 6, par. 1, lett. e) e 10 GDPR [126]. Sebbene nessuna delle due disposizioni vieti che una legge nazionale autorizzi o imponga a un'autorità pubblica di comunicare dati personali a coloro che ne fanno richiesta, tale normativa deve non solo essere necessaria per l'esecuzione di un compito di interesse pubblico, ma deve anche prevedere garanzie adeguate per i diritti e le libertà degli interessati. Nel caso di specie, secondo i giudici di Lussemburgo, l'obbligo di comunicazione previsto dalla legge finlandese in base all'art. 86 GDPR [127] rappresenta un'ingerenza grave nei diritti sanciti dagli artt. 7 e 8 della Carta, e questi ultimi devono prevalere poiché: i) i dati comunicati (ossia relativi a condanne penali di una persona fisica) sono dotati di una natura particolarmente sensibile *ex* art. 10 GDPR [128]; ii) il diritto alla libertà d'informazione non giustifica la comunicazione di tali dati a qualsiasi persona che ne faccia richiesta, senza che vi sia un interesse specifico a ottenere tali dati [129].

Nel giungere a questa conclusione, quello che sorprende maggiormente è la mancanza di una valutazione effettiva sul modo in cui la legge finlandese in materia di trasparenza della pubblica amministrazione soddisfa o meno i requisiti fissati dall'art. 6, par. 3, GDPR e dall'art. 52, par. 1, Carta [130]. In particolare, la Corte non esamina se: i) la normativa nazionale è idonea a soddisfare l'interesse pubblico di consentire l'accesso al pubblico ai documenti ufficiali; ii) esiste una misura meno pregiudizievole per i diritti degli interessati che consenta di realizzare i medesimi obiettivi; iii) la normativa nazionale è proporzionata *stricto sensu* ai fini della realizzazione degli obiettivi perseguiti. Questo tipo di approccio interpretativo presenta varie criticità [131].

---

[126] Per una ricostruzione dei fatti della causa, si rimanda a quanto descritto nella sezione 2.1.

[127] Sulla base di tale disposizione, "i dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento".

[128] Sentenza *Endemol*, punto 54.

[129] *Ibid.* punto 56.

[130] Sul punto, la giurisprudenza della Corte è pacifica nel ritenere che il diritto dell'Unione o dello Stato che costituisce la base giuridica del trattamento dei dati ai sensi dell'art. 6, par. 1, lett. c) ed e), GDPR deve soddisfare, ai sensi dell'art. 6, par. 3, GDPR, specifici requisiti, i quali sono espressione dei criteri di cui all'art. 52, par. 1, Carta (sentenze *Commissione c. Polonia (Indipendenza e privacy dei giudici)*, punto 337 e *Vyriausioji tarnybinės etikos komisija*, punto 69). In particolare, la normativa in questione deve perseguire un obiettivo di interesse generale e deve essere proporzionata all'obiettivo legittimo perseguito (*Vyriausioji tarnybinės etikos komisija*, punto 73).

[131] S. LINDROOS-HOVINHEIMO, *Op-Ed: The Principle of Openness Gives Way to Data Protection. Judgment in Case C-740/22 Endemol Shine*, in *Eu Law Live*, 2024.

Più precisamente, preme sottolineare che la scarna motivazione fornita dai giudici solleva dubbi sul modo in cui gli Stati membri possano legittimamente sfruttare il margine di discrezionalità concesso dal GDPR per conciliare il diritto fondamentale alla protezione dei dati personali con altri diritti che possono assumere rilievo anche costituzionale all'interno di un ordinamento nazionale (ad es. diritto di accesso ai documenti pubblici, libertà di espressione e d'informazione, diritto alla salute) [132]. Le disposizioni come quelle analizzate sopra sono state concepite proprio per consentire un bilanciamento che, qualora dovesse risolversi a favore del diritto alla protezione dei dati personali, dovrebbe comunque essere il risultato di un'attenta valutazione delle posizioni meritevoli di tutela coinvolte.

A questo proposito, vale la pena ricordare anche l'art. 85 GDPR, che consente agli Stati membri di prevedere esenzioni e deroghe al diritto alla protezione dei dati personali in casi di trattamento a fini esclusivamente giornalistici. Tale disposizione è stata fortemente voluta dal Consiglio [133] dopo la sentenza *Google Spain* [134]. In quella occasione, infatti, la Corte, discostandosi dalle conclusioni dell'Avvocato generale Jääskinen [135], ha stabilito che il

---

[132] Nel caso di specie, l'obbligo di comunicazione dei dati contenuti in documenti pubblici previsto dalla legge finlandese è stato introdotto, ai sensi dell'art. 86 GDPR, per fornire un'adeguata tutela al diritto di accesso del pubblico ai documenti ufficiali, riconosciuto dall'art. 12 della Costituzione finlandese quale espressione della libertà d'informazione. Nel capitolo 2 della Costituzione finlandese del 1999, rubricato "*basic rights*", l'art. 12 afferma che "*[d]ocuments and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings*".

[133] Nel corso del lungo iter che ha portato all'adozione del GDPR, gli Stati membri hanno infatti espresso la necessità che la nuova normativa fosse in grado di assicurare un equilibrio adeguato tra il diritto fondamentale alla protezione dei dati e la libertà di espressione, in particolare in un contesto digitale (Comunicato stampa 336ª sessione del Consiglio Giustizia e affari interni Lussemburgo, 9 e 10 ottobre 2014).

[134] Sentenza *Google Spain*. Per un commento alla sentenza, si rinvia B. ZELGER, *The Right to Be Forgotten in the European Union: Towards a Uniform Approach*, in *GPLR*, 2022, vol. 3, n. 1, pp. 19-28; I.S. GENANNT DÖHMANN, *A New Framework for Information Markets: Google Spain*, in *CMLRev.*, 2015, vol. 52, n. 4, pp. 1033-1057; D. ERDOS, *From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection*, in *CMLRev.*, 2015, vol. 52, n. 1, pp. 119-153.

[135] Conclusioni dell'Avvocato generale Jääskinen del 25 giugno 2013, causa 131/12, *Google Spain*, ECLI:EU:C:2013:424. L'Avvocato generale dichiara che la DPD non riconosce un "diritto all'oblio generalizzato" da invocare nei confronti di fornitori di servizi di motore di ricerca su Internet, basato su una mera "preferenza soggettiva", anziché su "un motivo preminente e legittimo" (punti 108 e 109). Secondo l'Avvocato generale, il riconoscimento di un simile diritto all'oblio che rafforza la posizione giuridica della persona interessata è impedito dalla "costellazione particolarmente complessa e difficile di diritti fondamentali".

diritto personalistico alla deindicizzazione (diritto all'oblio) deve prevalere sui legittimi interessi del gestore del motore di ricerca nonché sul generale interesse all'informazione [136].

Simili intenti, pur non derivando da pronunce della Corte, hanno portato all'introduzione dell'art. 89 GDPR, che permette agli Stati membri di prevedere deroghe ai diritti degli interessati (ad es. il diritto di accesso, rettifica, limitazione del trattamento e opposizione) in caso di trattamento di dati personali per fini di ricerca scientifica *ex* art. 9, par. 2, lett. j), GDPR. In presenza di adeguate garanzie, il legislatore europeo ammette in queste ipotesi un alleggerimento degli oneri a carico dei titolari del trattamento, riconoscendo le potenzialità che l'uso dei dati per scopi di ricerca scientifica può avere non solo per i titolari stessi, ma anche per l'intera collettività. Oltre a un interesse di natura commerciale, infatti, questa tipologia di trattamenti può realizzare interessi pubblici, come l'avanzamento della ricerca per la cura di determinate patologie o lo sviluppo di tecnologie sanitarie innovative [137].

In conclusione, sebbene il GDPR cerchi in vari modi di tutelare sia la posizione giuridica degli interessati sia quella dei titolari del trattamento, le sentenze della Corte sembrano privilegiare le prerogative dei primi. Questo approccio risulta problematico soprattutto in assenza di un bilanciamento effettivo tra i diritti fondamentali in gioco [138], tramite un'applicazione sistematica del principio di proporzionalità. Senza differenze significative tra il periodo precedente e successivo all'entrata in vigore del Trattato di Lisbona, né tra quello antecedente e conseguente al GDPR, dalle pronunce sino ad ora analizzate emerge come la Corte abbia interpretato e continui a interpretare la normativa sui dati personali al (solo) fine di garantire un grado elevato di tutela alle persone fisiche rispetto al trattamento dei loro dati personali. Ciò ha portato, da un lato, a estendere il campo di applicazione di questa disciplina, rendendolo sostanzialmente illimitato e, dall'altro, a conferire al diritto alla protezione dei dati personali lo status di "(super) diritto fondamentale

---

In particolare, "ciò vorrebbe dire sacrificare diritti primari come la libertà di espressione e di informazione" (punto 133).

[136] Sentenza *Google Spain*, punto 97

[137] Questo aspetto verrà approfondito nel capitolo 4.

[138] Al contrario, nel caso di specie (*Google Spain*), l'Avvocato generale Jääskinen ha interpretato le norme della DPD, prendendo in considerazione non solo i diritti alla protezione dei dati personali e al rispetto della vita privata, ma anche "le libertà di espressione e di informazione, come tutelate dall'articolo 11 (entrambe con riferimento alla libertà di espressione degli editori di pagine web e alla libertà degli utenti di Internet di ottenere informazioni), e la libertà di impresa, prevista all'articolo 16", dal momento che "i diritti delle persone interessate previsti agli articoli 7 e 8 debbono essere ponderati con i diritti, garantiti agli articoli 11 e 16, di quanti intendono diffondere i dati o avervi accesso" (punto 103).

assoluto" [139], minando così l'efficacia di quelle disposizioni che consentirebbero di conciliare quest'ultimo con altri diritti e interessi meritevoli di tutela.

3. Verso un equilibrio maggiormente in linea con gli obiettivi strategici del legislatore europeo

Il radicarsi di un approccio interpretativo della disciplina europea sui dati come quello descritto nella sezione precedente ha il pregio di assicurare un eccezionale livello di tutela alle prerogative degli interessati, il che rappresenta un *unicum* nel panorama normativo globale [140]. La garanzia di un simile standard di protezione è di cruciale importanza, soprattutto in contesti caratterizzati da forti asimmetrie informative, dove gli interessati si trovano in

[139] Conclusioni dell'Avvocato generale Bobek del 2 settembre 2021, causa C-175/20, *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, ECLI:EU:C:2021:690, punto 2. In questi termini si è espresso anche l'Avvocato generale Szpunar dell'11 maggio 2023, causa C-33/22, *Österreichische Datenschutzbehörde c. WK*, ECLI:EU:C:2023:397, punto 64, affermando che "il diritto delle persone fisiche alla protezione dei dati personali […] riveste un'importanza *speciale* rispetto agli altri diritti fondamentali che hanno trovato la loro collocazione nella Carta allegata al Trattato" (corsivo aggiunto). L'idea secondo cui il diritto alla protezione dei dati personali avrebbe progressivamente assunto i tratti di un "diritto assoluto" deriva da un orientamento interpretativo consolidato della Corte, che tende a tutelarlo in modo tale da non lasciare spazio a un effettivo bilanciamento con altri diritti fondamentali (v. per tutti la sentenza *Google Spain*). La qualificazione del diritto alla protezione dei dati personali come "assoluto" va quindi intesa in senso funzionale, ossia come diritto di fatto non bilanciabile, più che come diritto assoluto in senso tecnico-giuridico. Per chiarire, i diritti assoluti in senso stretto sono quelli che non ammettono alcuna limitazione, nemmeno in presenza di interessi pubblici rilevanti o di altri diritti fondamentali. Un esempio paradigmatico è il divieto di trattamenti inumani e degradanti sancito all'art. 4 della Carta dei diritti fondamentali dell'Unione. Il carattere assoluto di tale diritto è stato riconosciuto dalla Corte di giustizia nella causa *Aranyosi e Căldăraru*, dove si è ritenuto legittimo rifiutare l'esecuzione di un mandato d'arresto europeo qualora sussista un rischio reale che la persona consegnata possa essere sottoposta a condizioni detentive contrarie all'art. 4 della Carta (sentenza della Corte del 5 aprile 2016, cause riunite C-404/15 e C-659/15 PPU, *Pál Aranyosi e Robert Căldăraru*, ECLI:EU:C:2016:198, punti 85-88). Nel caso del diritto alla protezione dei dati personali, non si è dunque in presenza di un diritto intrinsecamente assoluto, ma l'effetto combinato di un'interpretazione estensiva del suo ambito applicativo e di un livello particolarmente elevato di tutela riconosciuto dalla giurisprudenza ha finito per conferirgli un carattere assoluto, rendendo nei fatti estremamente complesso – se non impossibile – il bilanciamento con altri diritti fondamentali, quali la libertà di espressione e informazione (art. 11 Carta) e la libertà d'impresa (art. 16 Carta).

[140] A questo proposito, vi è in dottrina chi ritiene di poter parlare di "fortezza europea dei dati personali" (O. POLLICINO, *Judges, Privacy and Data Protection from a Multilevel Protection Perspective*, in *federalismi.it*, 2022, vol. 4, p. 820).

posizione di svantaggio rispetto ai titolari del trattamento, o quando il trattamento dei dati personali può generare effetti discriminatori nei confronti delle persone fisiche da cui i dati provengono.

Al tempo stesso, tuttavia, le interpretazioni estensive e talvolta manipolative [141] del GDPR e, ancor prima, della DPD, contribuiscono a diffondere una sorta di "terrorismo" [142] della protezione dei dati personali tra coloro che operano in questo settore. Anche i titolari del trattamento più diligenti, infatti, raramente possono considerarsi al riparo da potenziali contestazioni sulla liceità delle proprie attività. Essi devono dimostrare la conformità alle disposizioni del GDPR tramite l'adempimento di numerosi obblighi [143], che – specialmente nel momento in cui trattano dati sensibili – comportano il dispendio di risorse, tempo e conoscenze che non sempre sono disponibili [144]. Questo aspetto risulta ancor più evidente se si considera che gli oneri a carico dei titolari del trattamento sono diventati particolarmente gravosi a causa della più ampia portata del principio di "responsabilizzazione" (o *accountability*) [145] nel GDPR rispetto

---

[141] Termine utilizzato da De Gregorio in riferimento all'interpretazione fornita dalla Corte in *Schrems* (v. G. DE GREGORIO, *The Rise of Digital Constitutionalism in the European Union*, in *Int. J. Const. Law*, 2021, vol. 19, p. 54), e da Pollicino e Bassini con riguardo alla sentenza *Google Spain* (cfr. O. POLLICINO, M. BASSINI, *Art. 8 Carta dei diritti fondamentali dell'Unione europea*, in R. D'ORAZIO et al. (a cura di), *Codice della Privacy e Data Protection*, Giuffrè, Milano, 2021, p. 48).

[142] A. Fiorentini, *op. cit*., 2024, p. 864.

[143] Artt. 24 ss. GDPR. In breve, prima di iniziare qualsiasi attività di trattamento, i titolari devono accertarsi di: i) disporre di una base giuridica legittima, tra quelle elencate dall'art. 6 GDPR e/o dall'art. 9 GDPR; ii) rispettare i principi di cui all'art. 5 GDPR; ed iii) eseguire, una volta iniziate le operazioni di trattamento, un monitoraggio continuo del rispetto dei principali requisiti richiesti dalla normativa (ad es. art. 35 ss. GDPR).

[144] Conclusioni dell'Avvocato generale Pikamäe del 31 marzo 2022, causa C-77/21, *Digi*, ECLI:EU:C:2022:248, punto 46.

[145] Art. 5, par. 2, GDPR, concretizzato dagli artt. 24 e 32 GDPR (cfr. sentenza *Russmedia Digital*, punto 113; sentenze del 25 gennaio 2024, causa C-687/21, *MediaMarktSaturn*, ECLI:EU:C:2024:72, punto 43; del 14 dicembre 2023, causa C-340/21, *Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986, punto 57; sentenza *RW c. Österreichische Post AG*, punto 49; sentenza del 27 ottobre 2022, causa C-129/21, *Proximus*, ECLI:EU:C:2022:833, punti 79 ss.; sentenza *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, punto 77). Inizialmente formulato dall'Organizzazione per la cooperazione e lo sviluppo economico del 1980 (art. 14 linee guida dell'OCSE sulla protezione della privacy e sui flussi transfrontalieri di dati personali), il principio di *accountability* è annoverato tra i principi previsti dall'art. 5 GDPR (si veda anche l'art. 35 e i considerando 74-77), ed è alla base di numerosi documenti europei, tra cui gli Orientamenti etici per un'IA affidabile del Gruppo indipendente di esperti ad alto livello sull'Intelligenza Artificiale, 2019. Sulla difficoltà definitoria di questo principio, si vedano il parere del WP n. 03/2010 sul principio di responsabilità, WP173, 2010, p. 7 e le linee guida dell'EDPB n. 07/2020 sui concetti di titolare e responsabile del trattamento ai sensi del GDPR, 2021, p. 9. Dalla dottrina emerge un concetto di *accountability* come forma

alla DPD [146]. Secondo questo principio [147], i titolari del trattamento devono adottare comportamenti proattivi per garantire il rispetto della disciplina europea e al contempo dimostrare la conformità a essa [148].

Qualora non si riuscisse ad allegare quanto richiesto, le possibili conseguenze sanzionatorie sono significative, specialmente se confrontate con quelle previste dalla disciplina precedente [149]. Di conseguenza, nella pratica,

---

di responsabilità rafforzata. In particolare, G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 2019(a), vol. 1, p. 185 offre una definizione multiforme di *accountability* in termini di "obbligo di chi prenda delle decisioni e operi delle scelte di: 1) giustificarle dinanzi a coloro che di tali scelte subiscono gli effetti ed eventualmente 2) debbano, non solo rendere il conto per le scelte fatte, ma debbano anche 3) rispondere nelle sedi opportune (responsabilità politica, civile, penale, amministrativa, deontologica, sociale) per loro eventuali fallimenti e mancanze". In G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it*., 2019, p. 1676, il principio di *accountability* viene definito come "meccanismo a due livelli: da un lato, l'attuazione di misure e procedure, dall'altro lato, la conservazione delle relative prove". Sulla definizione di tale principio, si veda anche L. CALIFANO et al., *op. cit.*, 2023, p. 138 ss.; R. BECKER et al., *Purpose Definition as a Crucial Step for Determining the Legal Basis under the GDPR: Implications for Scientific Research*, in *JLB*, 2024, pp. 2-3; J. MÍŠEK, *Data Protection as Performance-Based Regulation*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022, p. 58 ss.; G. ZANFRIN-FORTUNA, *Article 16 TFEU – Commentary*, in H-J. BLANKE, S. MANGIAMELI (eds.), *The Treaty on the Functioning of the European Union. A Commentary*, Springer, Berlin, 2021, p. 425; G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contratto e impresa. Dialoghi con la giurisprudenza civile e commerciale*, 2020, vol. 2, pp. 713-731; G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ*., 2017, p. 10 ss.

[146] Art. 5, par. 2, DPD affermava solamente che "[i]l responsabile del trattamento è tenuto a garantire il rispetto delle disposizioni del paragrafo 1", senza specificare la necessità di dare prova della conformità a tali principi. Si veda anche la differente formulazione dell'art. 23, par. 2, DPD e dell'art. 24 GDPR sulla responsabilità del titolare del trattamento.

[147] D. BUTIN, M. CHICOTE, D. LE MÈTAYER, *Strong Accountability: Beyond Vague Promises*, in S. GUTWIRTH, R. LEENES, P. DE HERT (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer, Berlin, 2014, p. 343.

[148] P. HUSTINX, *The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, in Collected Courses of the European University Institute's Academy of European Law*, OUP, Oxford, 2013, p. 32.

[149] Il regime sanzionatorio imposto dagli artt. 83-84 GDPR ha infatti subìto un inasprimento rispetto a quello fissato dall'art. 24 DPD. Cfr. P. DE HERT, *EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPR in the Spirit of Cooperative Federalism*, in S. MONTALDO, F. COSTAMAGNA, A. MIGLIO (eds.), *EU Law Enforcement. The Evolution of Sanctioning Powers*, Routledge, New York, 2021, p. 291. Inoltre, rispetto alla DPD, il GDPR ha rafforzato gli strumenti per assicurare l'efficacia delle sue disposizioni in caso di violazione. Oltre ad aumentare le funzioni delle autorità di controllo (v. Capo VI GDPR), ha previsto una vasta gamma di strumenti per la tutela dei diritti degli interessati. Questi ultimi possono presentare reclami davanti a un'autorità di controllo (art. 77 GDPR) o esercitare un ricorso giurisdizionale contro un'autorità di controllo o un titolare del trattamento (art. 79 GDPR), nonché richiedere un risarcimento del danno, materiale o immateriale, subìto

il timore di eventuali contestazioni da parte delle autorità di controllo o dei responsabili della protezione dei dati (i famigerati DPO) [150] induce i titolari a adottare comportamenti eccessivamente prudenti, assimilabili alle pratiche di medicina difensiva [151]. Sulla base di un'analisi costi-benefici, i titolari spesso scelgono di non utilizzare i dati a loro disposizione, rinunciando preventivamente alla possibilità di condurre attività di trattamento [152], anche se giustificate da finalità di interesse generale.

---

in conseguenza di una violazione (art. 82 GDPR), senza dover dimostrare il superamento di "una soglia di rilevanza" per far valere tale diritto (sentenze della Corte del 4 settembre 2025, causa C-655/23, *Quirin Privatbank*, ECLI:EU:C:2025:655, punto 58; del 4 maggio 2023, causa C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370, punto 51; e sentenza *Agentsia po vpisvaniyata*, C-200/23, punti 147 e 149). A ciò si aggiunge l'art. 80, che consente l'avvio di azioni di rappresentanza da parte di determinati organismi, come associazioni per la tutela dei consumatori. La Corte ha riconosciuto a tali soggetti la legittimazione ad agire per violazioni del GDPR nella sentenza del 28 aprile 2022, causa C-319/20, *Meta Platforms I*, ECLI:EU:C:2022:322, orientamento poi confermato, successivamente, nella sentenza dell'11 luglio 2024, causa C-757/22, *Meta Platforms Ireland (Action représentative)*, ECLI:EU:C:2024:598.

[150] Figura introdotta dagli artt. 37-39 GDPR.

[151] Come è noto, tali pratiche sono comunemente identificate in letteratura alla stregua di comportamenti commissivi, come l'esecuzione di trattamenti non necessari e costosi (medicina difensiva positiva), od omissivi, ad esempio la mancata esecuzione di interventi complessi da parte del medico, deviando dall'originario fine di tutela del paziente e puntando piuttosto a evitare o a ridurre i rischi di azioni risarcitorie per presunte negligenze professionali (medicina difensiva negativa). Per una definizione di medicina difensiva, cfr. relazione del decreto Balduzzi (d.l. 13 settembre 2012, n. 189, Disposizioni urgenti per promuovere lo sviluppo del Paese mediante un più alto livello di tutela della salute, in G.U. 13 settembre 2012, n. 214) che descrive tale pratica come "l'insieme di atti e comportamenti posti in essere al fine di evitare i possibili contenziosi, inficiando conseguentemente la garanzia di una tutela piena ed effettiva della salute dei cittadini e determinando l'incremento dei costi a carico del Servizio sanitario nazionale [a causa della] prescrizione di esami diagnostici inappropriati, con gravi conseguenze sia sulla salute dei cittadini, sia sull'aumento delle liste di attesa e dei costi a carico delle aziende sanitarie".

[152] Simili effetti dissuasivi sono stati messi in luce dall'Avvocato generale Campos Sánchez-Bordona in riferimento alla possibilità di ottenere un risarcimento *ex* art. 82 GDPR, indipendentemente dall'esistenza di un danno, ma per la sola violazione della disciplina in questione. Una simile ipotesi "stimolerebbe probabilmente le controversie civili, con azioni magari non sempre giustificate, e potrebbe quindi disincentivare l'attività di trattamento dei dati" (conclusioni dell'Avvocato generale Campos Sánchez-Bordona del 6 ottobre 2022, causa C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2022:756, punto 55, che sono state accolte, in riferimento a questo specifico punto, anche dalla Corte nella stessa causa al punto 33. Al contrario, la Corte non ha seguito l'orientamento espresso dall'Avvocato generale relativamente alla necessità di provare il superamento di una certa soglia di gravità per far valere un danno immateriale conseguente a una violazione dei dati. Secondo i giudici, infatti, il diritto al risarcimento di un danno immateriale non è subordinato all'entità dei danni derivanti dalla violazione del GDPR, senza tuttavia eliminare l'obbligo per l'interessato di dimostrare di aver subìto "conseguenze negative"). Sul tema relativo all'effetto deterrente delle sanzioni comminate dalle

La percezione diffusa del GDPR come un "*roadblock*" per le attività di trattamento e condivisione dei dati personali [153], insieme all'adozione di pratiche difensive da parte dei titolari del trattamento che possono tradursi in una riduzione del benessere sociale complessivo, contrasta con gli obiettivi perseguiti dagli atti della Strategia europea per i dati e, in ambito sanitario, dallo EHDS. Quest'ultimo, come vedremo, mira a favorire l'uso dei dati sanitari a beneficio dei pazienti stessi e della collettività, in parte replicando il modello regolatorio del GDPR e in parte superandolo (sezione 3.1). L'analisi delle novità introdotte dallo EHDS con riferimento all'uso dei dati sanitari elettronici ci permetterà di individuare soluzioni interpretative alternative del GDPR che consentano non solo di assicurare maggiore coerenza tra il GDPR e lo EHDS, ma anche di realizzare appieno i "veri" obiettivi del GDPR (sezione 3.2).

3.1. Le scelte del legislatore nell'ambito dello spazio europeo dei dati sanitari

Lo EHDS si ispira sotto diversi aspetti (ad es. definitori, sostanziali e istituzionali) al modello regolatorio del GDPR, tanto che in dottrina alcuni autori hanno cominciato a parlare di un vero e proprio fenomeno di "*mimesis*" del GDPR [154]. A livello sostanziale, questo modello si traduce nella previsione di norme che, da un lato, attribuiscono agli interessati diritti individuali di

---

autorità, cfr. Y. BOCONG, L. JIANNAN, *The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation*, in *Int. J. Environ. Res. Public Health*, 2019, vol. 16, n. 6, p. 2.

[153] G. COMANDÉ, G. SCHNEIDER, *It's Time Leveraging the GDPR to Shift the Balance Towards Research-Friendly EU Data Spaces*, in *CMLRev.*, 2022, vol. 59, p. 746. Similmente, B-J. KOOPS, *op. cit.*, 2014, p. 11, il quale sottolinea che *"[m]any controllers see data protection law as a traffic light that is usually red or else a warning yellow (or orange, depending on the country), but seldom green. The misconception that data protection law only* restricts, *and not also* enables*, is widespread, and of the two functions of data protection–protecting fundamental freedoms and stimulating the free flow of personal data–the latter is often overlooked*".

[154] Cfr. V. PAPAKONSTANTINOU, P. DE HERT, *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of "Act-ification", "GDPR Mimesis" and "EU Law Brutality"*, in *TechReg*, 2022, pp. 52-56 e V. PAPAKONSTANTINOU, *The "Act-ification" of EU Law: The (Long-Overdue) Move Towards "Eponymous" EU Legislation*, in *Eu Law Blog*, 2021. Per alcune considerazioni critiche circa la non perfetta sovrapponibilità del modello inaugurato dal GDPR con quello delineato dallo EHDS – in particolare sotto il profilo istituzionale – si rinvia a A. FIORENTINI, *Rethinking the Institutional Framework for the EU Data Regulations: Towards an Enhanced Administrative Integration*, in *REALaw*, 2025, vol. 18, n. 3, pp. 51-79.

controllo (ad es. il diritto di accesso e il diritto alla portabilità) [155] e, dall'altro, stabiliscono regole che permettono il trattamento legittimo dei dati personali da parte dei titolari del trattamento (ad es. i principi *ex* art. 5 GDPR). Analogamente, il legislatore dello EHDS ha introdotto disposizioni che conferiscono alle persone fisiche/pazienti diritti individuali di controllo sui loro dati sanitari elettronici personali, oltre a una serie di norme che disciplinano l'utilizzo e la condivisione di tali dati.

L'intento, in continuità con il GDPR [156], è garantire l'autonomia decisionale delle persone fisiche e, al contempo, massimizzare i benefici economici e sociali derivanti dall'utilizzo e dalla condivisione dei dati sanitari per i pazienti stessi e la collettività, tramite l'attribuzione di diritti di controllo specifici, la cui portata può essere limitata dagli Stati membri (sezione 3.1.1). Inoltre, rispetto al GDPR, il bilanciamento tra le prerogative degli interessati e quelle dei titolari dei dati o degli utenti [157] viene reso possibile tramite l'introduzione di garanzie ulteriori per le persone fisiche (sezione 3.1.2).

A fronte di queste novità, metteremo in evidenza come l'adozione di un approccio interpretativo simile a quello affermatosi con il GDPR nella lettura dello EHDS non solo rischia di compromettere il raggiungimento dei suoi ambiziosi obiettivi, ma – in virtù della presenza di garanzie aggiuntive specifiche per il settore sanitario – non è nemmeno giustificato dalla necessità di assicurare una tutela rafforzata alle persone fisiche rispetto al trattamento dei loro dati sanitari.

---

[155] Sulla funzione dei diritti degli interessati per accrescere il loro controllo sui dati, cfr. O. LYNSKEY, *Deconstructing Data Protection: the 'Added-value' of a Right to Data Protection in the EU legal Order*, in *Int. and Comp. Law Quart*., 2014, vol. 63, p. 595; G. ZANFIR-FORTUNA, *Forgetting about Consent. Why the Focus Should be on 'Suitable Safeguards*, in *Data Protection Law*, in S. GUTWIRTH, R. LEENES, P. DE HERT (eds.), *op. cit*., 2014, p. 245; L. NAUDTS, P. DEWITTE, J. AUSLOOS, *op. cit*., 2022, p. 537.

[156] D'altronde, come è già ampiamente sottolineato nel capitolo 1, la base giuridica dello EHDS per quanto riguarda l'uso dei dati sanitari è la stessa del GDPR, ossia l'art. 16, par. 2, TFUE.

[157] Per evitare equivoci, si ricorda che la nozione di "titolari dei dati sanitari" ai sensi dell'art. 2, par. 2, lett. y), EHDS non coincide con quella di "titolari del trattamento" di cui all'art. 4, n. 7, GDPR, ma si avvicina maggiormente a quella di "titolari dei dati" contemplata all'art. 2, n. 8), DGA. I titolari dei dati sanitari, infatti, possono essere persone fisiche o giuridiche, autorità pubbliche, agenzie o altri organi nei settori della salute o dell'assistenza, nonché istituzione, organi, organismi e agenzie dell'Unione che hanno: i) il diritto o obbligo di trattare dati personali per l'erogazione di assistenza sanitaria o di cura o per scopi di sanità pubblica; ii) la capacità di rendere disponibili dati sanitari non personali attraverso il controllo della progettazione tecnica di un prodotto o di un servizio.

3.1.1. La tutela dei diritti individuali (di controllo)

Il primo degli obiettivi esplicitamente menzionati dallo EHDS è di migliorare l'accesso e il controllo delle persone fisiche sui propri dati sanitari elettronici, riconoscendo loro diritti individuali in relazione all'uso primario e secondario di tali dati [158]. Per raggiungere questo scopo, lo EHDS prevede un ampio catalogo di diritti per persone fisiche/pazienti, alcuni dei quali vanno a integrare quelli del GDPR [159], adattandoli alle specificità del settore sanitario, mentre altri vengono introdotti *ex novo*, senza una diretta corrispondenza nel GDPR [160].

Per quanto riguarda i primi, si pone particolare enfasi sul fatto che le persone fisiche possano esercitare questi diritti individuali di controllo facilmente, gratuitamente e rapidamente [161]. Questo è segnatamente importante nel settore sanitario, dove la tempestività nell'accesso e condivisione di dati accurati e completi può essere determinante per garantire il miglior trattamento possibile al paziente o la continuità delle cure. Per queste ragioni, nello EHDS, sono state introdotte rilevanti innovazioni rispetto al GDPR.

Il diritto di accesso ai dati sanitari elettronici, ad esempio, non riguarda più i soli dati detenuti dal titolare del trattamento, ma si estende a tutte le categorie di dati sanitari elettronici compresi nel campo di applicazione dello EHDS (in particolare, quelli elencati all'art. 14 EHDS) [162]. Questo diritto

---

[158] Considerando 1 e art. 1, par. 2, lett. a), EHDS.

[159] Il considerando 8 EHDS afferma espressamente che i diritti individuali previsti dallo EHDS integrano quelli previsti dal GDPR.

[160] A questi diritti si aggiungono quelli sanciti dal GDPR: il diritto alla revoca del consenso (art. 7, par. 3, GDPR), il diritto a ottenere informazioni (ad es. l'identità del titolare, le categorie di dati ed gli eventuali destinatari) (artt. 13-14 GDPR), il diritto alla cancellazione (art. 17 GDPR); il diritto di limitazione del trattamento e opposizione (rispettivamente, artt. 18 e 21 GDPR) e il diritto a non essere sottoposto a decisioni automatizzate (art. 22 GDPR). Questi diritti, ai sensi dell'art 6 EHDS, possono essere esercitati dalle persone fisiche anche online tramite i servizi di accesso ai dati (v. sezione 3.1.2). Sulla relazione tra i diritti previsti dal GDPR e quelli stabiliti nello EHDS, v. K.Ó. CATHAOIR, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

[161] In particolare, il diritto di accesso ai dati (art. 3 e considerando 9 EHDS). Cfr. art. 15 GDPR); il diritto di rettifica (art. 6 e considerando 13 EHDS. Cfr. art. 16 GDPR); il diritto a ricevere informazioni sull'accesso ai dati e sulle condizioni a cui i dati sono messi a disposizione per l'uso secondario (rispettivamente, art. 9 e considerando 16, e art. 58 considerando 66 EHDS. Cfr. artt. 12-14 GDPR); il diritto alla portabilità (art. 7 e considerando 14-15. Cfr. art. 20 GDPR).

[162] Per completezza espositiva, sebbene esuli dall'oggetto dell'analisi condotta nel presente capitolo, è opportuno ricordare che già la direttiva 2011/24/UE prevedeva il diritto ad una cartella clinica, scritta o elettronica, e all'accesso ad almeno una copia di tale cartella (art. 4, par. 2, lett. f)). Diritti che evidentemente lo EHDS contribuisce a rendere più chiari e precisi.

deve essere esercitato dalle persone fisiche non direttamente nei confronti del titolare, bensì tramite servizi di accesso ai dati [163], e richiede una risposta immediata [164]. Inoltre, come per il GDPR, anche nello EHDS, il diritto di accesso include la possibilità di ottenere una copia dei dati, che consiste però nella facoltà di scaricare gratuitamente una copia elettronica di (almeno) le categorie dei dati prioritarie (ad es. profili sanitari sintetici e prescrizioni elettroniche), nel formato di scambio delle cartelle cliniche elettroniche [165].

Ulteriori integrazioni e specifiche sono state apportate anche in merito al diritto alla portabilità. L'art. 20 GDPR si applica unicamente ai dati forniti direttamente dall'interessato (ad es. i dati anagrafici) [166], sulla base del consenso prestato o del contratto stipulato, e non obbliga il titolare del trattamento a rendere tecnicamente fattibile la trasmissione dei dati (ad es. in caso di assenza di interoperabilità tra i fornitori di assistenza sanitaria e la cartella clinica elettronica) [167]. Al contrario, il diritto alla portabilità previsto nello EHDS consente alla persona fisica di concedere l'accesso o di richiedere a un fornitore sanitario di trasmettere tutti o parte dei propri dati, compresi quelli *inferred* (ad es. la diagnosi), a un altro fornitore di assistenza sanitaria o a un destinatario chiaramente identificato nel settore della sicurezza sociale e dei servizi di rimborso [168]. Questo diritto include anche la facoltà di trasmettere una

---

[163] Art. 4 EHDS. Al contrario, il GDPR non specifica alcuna modalità particolare per fare in modo che l'interessato faccia pervenire al titolare la sua richiesta. Solamente il considerando 63 stabilisce che il diritto all'accesso ai dati, per essere effettivo, deve essere esercitato facilmente, senza quindi che il titolare imponga particolari modalità o oneri. Quest'ultimo può solamente suggerire alcune modalità di esercizio, ad esempio, predisponendo mezzi per inoltrare le richieste in via elettronica (considerando 59).

[164] Considerando 9 EHDS. Ai sensi del GDPR, invece, il titolare del trattamento ha un mese di tempo per rispondere alla richiesta di accesso ai dati (art. 12, par. 3 e considerando 59).

[165] Art. 3, par. 2, EHDS. Cfr. art. 15, parr. 3-4, GDPR.

[166] Il diritto alla portabilità può riguardare anche i dati connessi all'attività intrapresa dall'interessato tramite l'utilizzo di servizi o dispositivi, o i risultati derivanti dall'osservazione del suo comportamento. Sono invece esclusi i dati generati dal titolare attraverso processi specifici come la profilazione (ad es. il battito cardiaco registrato da un dispositivo) o quelli derivanti da un'attività svolta in modo autonomo dal titolare (ad es. i dati desunti). Cfr. Linee guida del WP sul diritto alla portabilità dei dati, WP 242, 2017.

[167] A questo proposito, vale la pena ricordare che il diritto alla portabilità dei dati previsto dal GDPR è stato definito in dottrina come "diritto di accesso con modalità vincolante" (V. FALCE, *Art. 20*, in R. D'ORAZIO et al., *op. cit.*, 2021, p. 351), in quanto consiste nel diritto di ricevere informazioni "in formato strutturato, di uso comune e leggibile da dispositivo automatico", ossia in un formato che consenta il riutilizzo dei dati (art. 20, par. 1, e considerando 68 GDPR).

[168] Art. 7, parr. 1-3, EHDS. Cfr. W. LI, P. QUINN, *The European Health Data Space: An Expanded Right to Data Portability?*, in *Comput. Law Secur. Rev.*, 2024, vol. 52, pp. 1-13 e W. LI, *The Right to Data Portability in the European Health Data Space: A Follow-up*, in *Health&Aging Law Lab*, 2024.

copia elettronica a un fornitore nel formato europeo di scambio delle cartelle cliniche elettroniche [169].

Per quanto riguarda i diritti introdotti *ex novo* dallo EHDS, i pazienti vengono dotati della facoltà di inserire dati, compresi quelli provenienti dalle applicazioni per il benessere [170], direttamente nella propria cartella clinica elettronica [171], e di limitare l'accesso dei professionisti e dei fornitori di assistenza sanitaria a tutti o parte dei dati (ad es. le informazioni relative a problemi connessi alla salute mentale o sessuale, l'aborto, l'assunzione di farmaci specifici) [172]. A questa stessa categoria appartengono anche i diritti di *opt-out* relativi all'uso primario e secondario dei dati sanitari elettronici, che si ispirano solo in parte al diritto di opposizione (*right to object*) del GDPR [173], differenziandosi per finalità e condizioni di esercizio.

In caso di uso primario dei dati, il diritto (reversibile) delle persone fisiche di opporsi all'accesso ai propri dati, registrati nella cartella clinica elettronica, da parte di terzi [174], implica che i dati rispetto a cui si è esercitato tale diritto

---

[169] Art. 7, par. 4, EHDS.

[170] Art. 48, par. 2, EHDS. Sui rischi connessi all'esercizio di tale diritto da parte dei pazienti e dei professionisti sanitari, si veda A.M. PHILLIPS, *The Right to Insert and Add Information to my Health Record – Does my Doctor Need to Know This? A Critical Discussion of the Right to Insert Information in an EHR Using the Example of Data from Direct-to-Consumer Genetic Testing*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

[171] Art. 5 e considerando 12 EHDS. Sempre nell'ottica di garantire l'esattezza e l'accuratezza delle informazioni all'interno della cartella clinica elettronica, lo EHDS stabilisce che i dati inseriti direttamente dai pazienti devono essere chiaramente distinguibili dagli altri, venendo collocati in una cartella personale separata. Questi dati possono essere consultati dai professionisti per integrare le informazioni a loro disposizione e, come detto, non hanno lo stesso valore clinico e legale di quelli inseriti dai professionisti, i quali non possono in alcun modo essere modificati dai pazienti.

[172] Art. 8 e considerando 17 EHDS. A questo proposito, lo EHDS specifica che le persone fisiche devono essere informate delle conseguenze che possono derivare dall'esercizio di tale diritto (ad es. i rischi per la sicurezza e il potenziale impatto sulla fornitura o la qualità dei servizi sanitari).

[173] Il diritto di opporsi al trattamento *ex* art. 21 GDPR prevede unicamente tre ipotesi di opposizione: i) il diritto di opporsi al trattamento di dati personali ai sensi dell'art. 6, par. 1, lett. e) e f), per motivi connessi alla situazione specifica dell'interessato (in questo caso, il titolare deve astenersi dal trattare ulteriormente i dati, salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato); ii) il diritto di opporsi al trattamento effettuato per finalità di *marketing* diretto; iii) il diritto di opporsi al trattamento condotto a fini di ricerca scientifica, a meno che tale trattamento sia necessario per l'esecuzione di un compito di interesse pubblico. Per un approfondimento sul rapporto tra il diritto di *opt-out* previsto dallo EHDS e il diritto di opporsi del GDPR, si rinvia a M. KRUUS, *Opting Out of Scientific Research with Health Data: The Limits of the EHDS and the GDPR*, in *EJHL*, 2025, pp. 1-25.

[174] Art. 10 EHDS.

non saranno resi accessibili tramite i servizi dell'EHDS, fatta eccezione per il professionista sanitario che ha fornito il trattamento iniziale. L'introduzione di questa possibilità mira a rispettare le diverse sensibilità nazionali in materia di controllo individuale sui dati sanitari [175]. Motivi analoghi hanno portato all'introduzione di un diritto di *opt-out* in caso di uso secondario dei dati, il quale, tuttavia, deve essere obbligatoriamente previsto dal diritto nazionale [176].

Come nel GDPR, i diritti riconosciuti dallo EHDS non sono assoluti, ma possono essere limitati. In conformità all'art. 23 GDPR [177], lo EHDS ammette la possibilità che gli Stati membri introducano restrizioni ai diritti delle persone fisiche per motivi specifici. Ad esempio, per quanto riguarda il diritto di accesso, una normativa nazionale può consentire al professionista sanitario di ritardare per un tempo limitato l'accesso ai dati quando la visualizzazione immediata degli stessi è dannosa per la sicurezza dei pazienti o non è etica. Si pensi al caso in cui il paziente, consultando la propria cartella clinica elettronica, scoprisse di essere affetto da una patologia incurabile. In quest'eventualità, l'accesso ai dati può essere ritardato fino a quando un professionista sanitario non sia in grado di comunicare e spiegare adeguatamente alla persona le informazioni aventi un impatto sulla sua salute [178].

Ulteriori limitazioni possono essere previste per il diritto alla condivisione selettiva dei dati ai professionisti sanitari, il diritto di ottenere informazioni e il diritto di *opt-out* all'uso primario al fine di tutelare gli interessi vitali del paziente [179], dell'operatore sanitario [180] o di terzi [181]. Anche con riferimento al diritto di *opt-out* per uso secondario, è possibile che, a livello nazionale, vengano introdotte delle ipotesi in cui i dati rispetto ai quali si è esercitato tale

---

[175] Considerando 18 EHDS.

[176] Art. 71 e considerando 54 EHDS. Cfr. T. SOKOL, *European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance*, in *EJHL*, 2024, vol. 4, pp. 365-388.

[177] Secondo l'art. 23 GDPR, le limitazioni ai diritti di cui agli artt. 12-21 GDPR, possono essere introdotte per salvaguardare motivi come la sicurezza nazionale, la difesa e la sicurezza pubblica, e devono: i) essere adottate con misure legislative; ii) rispettare l'essenza dei diritti e delle libertà fondamentali; iii) essere una misura necessaria e proporzionata in una società democratica. Il richiamo implicito è, ovviamente, all'art. 52 della Carta, tanto che il considerando 73 GDPR precisa che le limitazioni di cui all'art. 23 GDPR "dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali".

[178] Art. 3, par. 3 e considerando 10 EHDS.

[179] Art. 8 e considerando 17 EHDS.

[180] Art. 9 e considerando 16 EHDS.

[181] Art. 10 EHDS.

diritto possano essere messi a disposizione di un ente pubblico o un'istituzione, organo, organismo o agenzia dell'Unione affinché svolga attività nel settore della sanità pubblica o per motivi di interesse pubblico (ad es. le attività condotte per la protezione contro gravi minacce transfrontaliere alla salute o le ricerche scientifiche per importanti ragioni di interesse pubblico) [182].

La possibilità di prevedere limitazioni ai diritti delle persone fisiche rende evidente la scelta del legislatore di evitare che gli individui possano vantare diritti assoluti, inconciliabili con la tutela di altri diritti e interessi, preferendo piuttosto garantire loro la possibilità di esercitare varie forme di controllo sull'uso e sui dati stessi. Come vedremo per il GDPR, anche per lo EHDS è possibile classificare i diritti riconosciuti alle persone fisiche sulla base del tipo di controllo a loro conferito. In particolare, possiamo distinguere tra i diritti che consentono alle persone fisiche di monitorare la correttezza delle operazioni di trattamento aventi oggetto i propri dati (ad es. il diritto di accesso ai dati e il diritto di ottenere informazioni) e quelli che permettono loro di intervenire in modo "proattivo" sull'uso dei dati (ad es. il diritto di *opt-out* e il diritto a limitare l'accesso ai dati) e sui dati stessi (ad es. il diritto di rettifica, il diritto di inserire i propri dati nella cartella clinica e il diritto alla portabilità).

Le analogie tra le scelte operate dal legislatore dello EHDS e quelle del GDPR, unite alla necessità che lo EHDS rispetti l'*acquis* europeo in materia di protezione dei dati personali, potrebbero indurre l'interprete ad applicare alle disposizioni del nuovo regolamento lo stesso approccio ermeneutico consolidatosi con riferimento al GDPR. Tuttavia, interpretazioni che attribuiscono una tutela prioritaria alle prerogative degli interessati non solo, come sottolineeremo in seguito, tradiscono i "veri" obiettivi del GDPR [183], ma risultano anche disallineate rispetto al mutato contesto normativo in cui si inserisce l'EHDS. Quest'ultimo, infatti, pur rispettando il diritto individuale alla protezione dei dati personali, riconosce l'importanza di favorire l'uso dei dati, specialmente per interessi generali.

Mantenere un approccio interpretativo rigidamente orientato alla massima tutela individuale rischia di depotenziare l'impianto innovativo dello EHDS, in particolare le sue disposizioni volte a facilitare e semplificare l'uso e la

[182] Art. 71, par. 4, EHDS. Lo stesso articolo al paragrafo 5 specifica che il diritto nazionale che introduce queste limitazioni, da notificare alla Commissione, deve contenere misure specifiche e adeguate a proteggere i diritti fondamentali e i dati personali delle persone fisiche e disposizioni per la sicurezza e la protezione dei diritti delle persone fisiche. Inoltre, queste restrizioni non possono ledere l'essenza dei diritti e delle libertà fondamentali e devono essere necessarie e proporzionate in una società democratica per soddisfare l'interesse pubblico nel settore degli obiettivi scientifici e sociali legittimi.

[183] Si rinvia alla sezione 3.2 del presente capitolo.

condivisione dei dati sanitari elettronici. Ad esempio, un'interpretazione eccessivamente restrittiva della deroga al diritto di *opt-out* all'uso secondario comporta il rischio che, nell'assicurare alle persone fisiche il pieno controllo sui loro dati, si finisca per pregiudicare l'interesse degli utenti ad avere accesso a banche dati complete. La possibilità di accedere a dataset con queste caratteristiche soddisfa non solo l'interesse del singolo utente, ma anche quello della società nel suo complesso, che, tramite banche dati esaustive, può beneficiare di risultati accurati, rappresentativi e riproducibili [184].

Infine, applicare allo EHDS lo stesso paradigma interpretativo elaborato per il GDPR non sembra giustificato dall'esigenza di una protezione rafforzata per i dati sanitari. Lo EHDS, infatti, contiene già in sé le tutele e le garanzie adeguate a tal fine. Come evidenziato in precedenza, rispetto al GDPR, esso non solo amplia e specifica diritti di controllo fondamentali come il diritto di accesso e il diritto alla portabilità, ma introduce anche nuovi diritti a tutela dell'autonomia dell'interessato (ad es. il diritto di *opt-out*). Inoltre, in maniera del tutto innovativa, prevede un sistema di governance dei dati per l'uso primario e secondario che permette di bilanciare adeguatamente *ex ante* i diritti e gli interessi in gioco [185].

3.1.2. I servizi e gli organismi per l'accesso ai dati sanitari elettronici

Per facilitare l'uso primario e secondario dei dati sanitari elettronici da parte degli utenti (ad es. professionisti sanitari, ricercatori e responsabili delle politiche sanitarie), senza compromettere le prerogative degli interessati né aumentare gli oneri gravanti sui titolari dei dati, lo EHDS aggiunge un tassello importante alla disciplina europea per la protezione dei dati personali in ambito sanitario. Questo tassello consiste nell'istituzione di servizi di accesso ai dati per i pazienti e i professionisti sanitari, nonché nella designazione di organismi responsabili dell'accesso ai dati.

I servizi di accesso ai dati sono concepiti per assicurare l'effettività dei diritti delle persone fisiche, senza che il soddisfacimento delle loro richieste rappresenti un onere eccessivo per i titolari dei dati [186]. Similmente, gli

---

[184] Questo aspetto sarà evidenziato anche nella sezione 3.2.2, parlando degli effetti derivanti dalla revoca del consenso al trattamento dei dati personali.

[185] In questi termini, e con particolare riferimento al potenziale del controllo *ex ante* introdotto dallo EHDS quale meccanismo che rafforza le tutele rispetto al quadro del GDPR, cfr. A. PARZIALE, E. PULICE, D. MASCALZONI, *Mass-Scale G2B Data Sharing in an Emergency: Between the GDPR, Data Governance Act, and European Health Data Space*, in *European Journal of Health Law*, 2025, p. 30.

[186] Diversamente, per garantire l'effettività dei diritti individuali degli interessati, il GDPR impone ai titolari e ai responsabili del trattamento, tra le altre cose, di fornire gratuitamente

organismi responsabili dell'accesso ai dati dovrebbero fornire le garanzie necessarie affinché l'uso secondario dei dati sanitari avvenga nel rispetto del diritto individuale alla protezione dei dati personali, realizzando contemporaneamente l'interesse degli utenti a beneficiare degli stessi.

Più nello specifico, per quanto riguarda l'uso primario dei dati, lo EHDS richiede agli Stati membri di istituire uno o più servizi di accesso ai dati sanitari elettronici (ad es. portali online per i pazienti e applicazioni mobili) a livello nazionale, regionale o locale, resi disponibili gratuitamente [187]. Inoltre, devono essere forniti servizi di delega che consentano alle persone fisiche di autorizzare soggetti terzi ad accedere ai loro dati sanitari (o parte di questi) e ai rappresentanti legali di accedere ai dati sanitari delle persone fisiche di cui gestiscono gli affari [188]. Gli Stati membri devono anche istituire servizi di assistenza, con personale adeguatamente preparato, per aiutare le persone fisiche nell'esercizio dei loro diritti [189]. Tali servizi devono essere progettati in modo da essere accessibili, anche alle persone con disabilità, e devono prevedere sistemi di identificazione elettronica in linea con il nuovo regolamento (UE) 2024/1182 [190].

Come anticipato, l'introduzione di questa modalità di esercizio dei diritti, unica e vincolata, dovrebbe assicurare l'effettivo godimento dei diritti delle persone fisiche in caso di uso primario, superando le difficoltà riscontrate nella vigenza del GDPR [191]. Questo significa, ad esempio, che un paziente che desideri accedere, modificare o condividere con terzi dati contenuti nella propria cartella clinica elettronica non dovrà più necessariamente rivolgersi al titolare del trattamento, ma potrà esercitare direttamente (o mediante una

---

all'interessato informazioni chiare e trasparenti riguardo ai propri diritti e di predisporre un sistema di gestione delle richieste di esercizio di tali diritti da parte dell'interessato (art. 12 GDPR).

[187] Art. 4 e considerando 20 EHDS.

[188] Art. 4, par. 2, e considerando 21 EHDS.

[189] Considerando 21 EHDS. A questo proposito, la disciplina generale del DGA (art. 2, n. 15) prevede l'istituzione di servizi di intermediazione, tra cui quelli di cooperative di dati, volti a potenziare la capacità d'azione degli interessati e il loro controllo. Questi servizi, infatti, dovrebbero assistere gli interessati nell'esercizio dei loro diritti, occupandosi, ad esempio, della gestione della concessione e revoca del consenso al trattamento dei dati, nonché dei diritti di accesso, rettifica, cancellazione, limitazione del trattamento e portabilità (considerando 30-32 DGA).

[190] Art. 16 e considerando 20 e 21 EHDS. Il regolamento (UE) 2024/1182 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

[191] Sul punto, si rimanda all'analisi svolta della Commissione nella relazione di valutazione di impatto che accompagna la proposta di regolamento sullo Spazio europeo dei dati sanitari, SWD(2022) 131 final, di cui si è trattato nel cap. II, sezioni 2 e 5.

persona da lui designata) i propri diritti, avvalendosi dei servizi di accesso e di delega appena descritti.

Passando all'uso secondario dei dati sanitari elettronici, la principale innovazione rispetto all'impostazione del GDPR, in cui i soggetti coinvolti nel trattamento dei dati personali sono i titolari (o i responsabili) e gli interessati, è l'introduzione degli organismi responsabili dell'accesso ai dati [192]. Benché lo EHDS non fornisca una definizione specifica di tali organismi, essi sono sostanzialmente entità in grado di mettere a disposizione, a chi ne fa richiesta, i dati forniti dai titolari per l'uso secondario [193]. Con l'entrata in vigore dello EHDS, quindi, per utilizzare i dati sanitari elettronici per scopi diversi da quelli di assistenza sanitaria (ad es. interesse pubblico o ricerca scientifica in ambito sanitario) [194], in linea di principio sarà sufficiente rivolgersi agli organismi per l'accesso ai dati [195].

Questi ultimi sono responsabili, tra le altre cose, di decidere in merito alle domande di accesso ai dati o alle richieste di dati [196]. In particolare, quando

---

[192] Art. 55 EHDS. Per quanto riguarda il ruolo centrale degli organismi responsabili per l'accesso ai dati nella facilitazione e gestione della condivisione dei dati sanitari per usi secondari, cfr. T. PETROČNIK, *Secondary Use of Health Data in the EHDS: Public Interest and the Role of HDABs*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025 e J. REICHEL, *Administrative Tools for Balancing Social and Individual Interests. Data Protection Safeguards and Administrative Procedural Guarantees in Secondary Use in the European Health Data Space*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, pp. 217-220.

[193] Una definizione simile si allinea con quella proposta dal Parlamento europeo nel corso del dialogo interistituzionale con riferimento alle "entità di intermediazione dei dati", ma che non ha trovato accoglimento nel testo definitivo dello EHDS.

[194] In base all'art. 53 EHDS, i dati sanitari elettronici possono essere messi a disposizione per attività di pubblico interesse nell'ambito della sanità pubblica e della medicina del lavoro, di ricerca scientifica nel settore sanitario o dell'assistenza, nonché per attività di sviluppo e innovazione per prodotti o servizi che contribuiscono al miglioramento della sanità pubblica e di addestramento, prova e valutazione degli algoritmi, anche nell'ambito dei dispositivi medici, sistemi di IA e applicazioni di sanità digitale, e per l'erogazione di un'assistenza sanitaria personalizzata. Al contrario, ai sensi dell'art. 54 EHDS, è vietato l'uso secondario dei dati sanitari elettronici per l'adozione di decisioni pregiudizievoli per una persona fisica (ad es. l'esclusione dal beneficio di un contratto di assicurazione o la modifica dei premi assicurativi), per attività pubblicitarie o di *marketing* o per lo sviluppo di prodotti e servizi in grado di danneggiare le persone e la società in generale.

[195] Ai sensi dell'art. 56 EHDS, qualora i titolari di dati siano delle istituzioni, organi, organismi e agenzie dell'Unione, i compiti degli organismi per l'accesso ai dati spettano alla Commissione.

[196] Art. 57, par. 1, lett. a), EHDS. Oltre alle procedure di domanda di accesso ai dati (art. 68 EHDS) e di richiesta di dati (art. 69 EHDS), lo EHDS prevede altre due modalità di accesso ai dati: i) una procedura accelerata di accesso ai dati che può essere prevista dagli Stati membri, per gli enti pubblici e le istituzioni, organi, organismi e agenzie dell'Unione se il trattamento dei dati avviene per motivi di interesse pubblico, al fine di mettere i dati a loro

viene presentata una domanda di accesso ai dati, essi devono valutare che questa: i) soddisfi determinati requisiti (ad es. la conformità agli artt. 5 e 6 GDPR e l'attuazione di adeguate misure tecniche e organizzative per prevenire l'uso abusivo dei dati e per proteggere i diritti e gli interessi del titolare e delle persone fisiche coinvolte); ii) consenta di mitigare alcuni rischi (ad es. quelli legati alla difesa nazionale, sicurezza pubblica e ordine pubblico, o il rischio di compromettere la confidenzialità di dati presenti nei database governativi delle autorità regolatorie). Una volta rilasciata l'autorizzazione all'accesso ai dati, gli organismi richiedono immediatamente i dati al titolare e li forniscono all'utente [197], in forma anonimizzata o pseudonimizzata, all'interno di un ambiente sicuro di trattamento [198].

I compiti di controllo e supervisione affidati agli organismi responsabili dell'accesso ai dati nella valutazione delle domande di accesso ai dati e delle richieste di dati, unitamente alle condizioni di sicurezza per la messa a disposizione dei dati sanitari (di regola, anonimizzati) nell'ambiente sicuro di trattamento, rappresentano le garanzie fondamentali individuate dal legislatore europeo per assicurare che il loro uso per finalità secondarie avvenga nel rispetto dei valori dell'Unione e della disciplina europea sui dati personali.

Il coinvolgimento di figure "intermedie" tra i titolari/le persone fisiche e gli utenti rappresenta una scelta legislativa che si inserisce nella direzione tracciata dalla disciplina generale del DGA. Tra le altre cose, tale disciplina affida alle organizzazioni per l'altruismo dei dati il compito di gestire le condivisioni volontarie dei dati per finalità di interesse generale (ad es. assistenza sanitaria e ricerca scientifica). In particolare, le disposizioni sull'altruismo dei dati del

---

disposizione in un tempo inferiore a due mesi (art. 46, par. 3b, e considerando 52); ii) una procedura semplificata che si applica quando la domanda di accesso ai dati o la richiesta di dati riguarda solo dati detenuti da titolari di fiducia, designati dagli Stati membri qualora il titolare soddisfi alcune condizioni specifiche, tra cui la possibilità di fornire l'accesso ai dati in un ambiente sicuro di trattamento. Secondo tale procedura, le domande di accesso ai dati e le richieste di dati devono essere inviate all'organismo responsabile per l'accesso ai dati che le indirizza al titolare di fiducia, il quale deve effettuare le sue valutazioni e inviarle all'organismo. Quest'ultimo, nel prendere la sua decisione, non è in alcun modo vincolato dalla posizione espressa dal titolare di fiducia (art. 72 e considerando 76 EHDS).

[197] Agli utenti potrebbe essere richiesto di pagare una tariffa agli organismi per l'accesso ai dati così da consentire loro di coprire i costi (tutti o in parte) sostenuti per il fatto di aver messo a disposizione i dati, compresi quelli relativi alla consolidazione, preparazione, anonimizzazione, pseudonimizzazione dei dati, nonché quelli sostenuti dal titolare per aver compilato e preparato i dati da mettere a disposizione. In ogni caso, una riduzione delle tariffe potrebbe essere prevista per utenti determinati (ad es. enti del settore pubblico, istituzioni, organismi, organi e agenzie dell'Unione, ricercatori universitari). Cfr. art. 62 e considerando 70 EHDS.

[198] Art. 73 EHDS. Gli ambienti di trattamento sicuro devono rispettare una serie di requisiti di sicurezza, come l'accesso riservato esclusivamente al personale autorizzato.

DGA permettono di mettere in evidenza la scelta del legislatore europeo di assicurare l'autonomia e il coinvolgimento degli individui nell'uso dei propri dati, senza tuttavia privare la collettività dei benefici ad essi connessi.

In primo luogo, l'altruismo dei dati personali, inclusi quelli sanitari, richiede il consenso degli interessati [199]. A tal fine, per semplificare la raccolta dei dati per finalità di interesse generale, l'art. 25 DGA autorizza la Commissione ad adottare atti di esecuzione per l'istituzione e l'elaborazione di un modulo europeo di consenso all'altruismo dei dati. Quest'ultimo utilizza un approccio "modulare" che ne permette la personalizzazione a seconda dei settori e delle finalità, e consente agli interessati di dare o revocare il proprio consenso rispetto all'utilizzo dei propri dati.

In secondo luogo, le organizzazioni per l'altruismo dei dati devono iscriversi in un registro pubblico nazionale, seguendo una procedura gestita da autorità competenti, le quali vigilano sulla conformità delle organizzazioni a requisiti specifici (ad es. lo svolgimento di attività di altruismo dei dati e l'indipendenza da qualsiasi entità che operi a scopo di lucro) [200]. Una volta riconosciute dalle autorità competenti per la registrazione, le organizzazioni per l'altruismo dei dati sono soggette a una serie di obblighi di trasparenza (ad es. la tenuta di registri e la redazione di una relazione annuale) [201], oltre che a obblighi specifici di tutela dei diritti degli interessati e dei titolari dei dati (ad es. il divieto di utilizzo dei dati per obiettivi diversi da quelli di interesse generale) [202].

L'approccio adottato con il DGA in riferimento alle pratiche di altruismo dei dati presenta analogie con quello previsto per la donazione delle sostanze di origine umana (SoHO) [203]. Anche il regolamento sulle SoHO richiede, infatti, il consenso dei donatori e la registrazione degli enti SoHO, ossia organizzazioni incaricate di supervisionare, coordinare e controllare le attività legate all'utilizzo delle SoHO a fini terapeutici o di ricerca [204]. Per garantire il

---

[199] Art. 2, n. 16, DGA. Diversamente, in caso di dati non personali, è necessario ottenere dai titolari dei dati non personali un'autorizzazione. Per un approfondimento sul punto, cfr. E. EL ASRY, J. MANSNÉRUS, S. LIEDE, *op. cit.*, 2025.

[200] Artt. 17-19 DGA. Al contrario, gli organismi per l'accesso ai dati sanitari elettronici vengono designati dagli Stati membri e non è necessario prevedere una registrazione specifica (art. 55 EHDS).

[201] Art. 20 DGA.

[202] Art. 21 DGA.

[203] Regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio, del 13 giugno 2024, sui parametri di qualità e sicurezza per le sostanze di origine umana destinate all'applicazione sugli esseri umani e che abroga le direttive 2002/98/CE e 2004/23/CE (regolamento SoHO).

[204] Art. 3, n. 33, regolamento SoHO.

rispetto delle norme etiche e di sicurezza, tali enti si occupano di proteggere i diritti, la sicurezza e il benessere delle persone coinvolte nel processo di utilizzo delle SoHO.

Nello specifico, gli enti SoHO vigilano sull'osservanza dei requisiti relativi al consenso, fornendo altresì ogni informazione necessaria sul processo di donazione e di raccolta, nonché sugli usi e sui potenziali benefici della donazione [205]. Inoltre, essi vigilano affinché sia rispettato il principio di donazione volontaria e gratuita [206], implicito nel divieto, previsto dall'art. 3, par. 2, Carta, di fare del corpo umano e delle sue parti in quanto tali una fonte di lucro [207]. Più precisamente, gli enti SoHO non possono offrire incentivi o vantaggi finanziari ai donatori [208]. Similmente, per le pratiche di altruismo dei dati non è ammessa la richiesta o l'accettazione di compensi che superino la mera copertura dei costi sostenuti per la condivisione dei dati [209].

Da queste considerazioni emerge che nei settori in cui la protezione degli individui richiede particolare attenzione, poiché sono in gioco diritti di rilievo costituzionale (ad es. i diritti previsti dagli artt. 3 e 8 della Carta), il legislatore europeo non ha scelto di vietare o limitare indiscriminatamente l'uso delle risorse "appartenenti" ai singoli (ad es. i dati personali e le SoHO). Al contrario, sembra esserci una tendenza normativa a privilegiare, accanto a forme di controllo più o meno intense, meccanismi e organismi intermedi che garantiscono l'utilizzo e la condivisione di queste risorse, per consentire a soggetti terzi e, più in generale, all'intera collettività di trarre vantaggio dal loro sfruttamento, senza compromettere la tutela dei diritti dei singoli.

---

[205] Artt. 52-55 regolamento SoHO. Si rimanda anche agli artt. 5 e 22 della Convenzione di Oviedo.

[206] Art. 53, par. 1, lett. d), regolamento SoHO.

[207] Questo divieto di commercializzazione delle parti del corpo è presente anche nell'art. 21 della Convenzione di Oviedo, dove si stabilisce che il corpo umano e le sue parti non possono essere fonte di profitto.

[208] Art. 54 regolamento SoHO.

[209] La logica di fondo è simile anche a quella alla base della dottrina dello "*sweat of the brow*" che si trova nel contesto del diritto d'autore o del "*substantial investment*" nella disciplina sulle banche dati (art. 7 direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati). Una scelta simile viene operata anche nel *Health Information Technology for Economic and Clinical Health (HITECH) Act* americano con riferimento alle richieste di dati per motivi di ricerca (42 U.S.C.A. § 17935(d)(2)(B)) e di sanità pubblica (42 U.S.C. § 17935(d)(2)(A) (2006)). Per un'analisi approfondita dell'*HITECH Act*, cfr. B.J. EVANS, *Much Ado About Data Ownership*, in *JOLT*, 2011, vol. 25, p. 109 ss.

3.2. I cambiamenti necessari nell'interpretazione del GDPR

Come anticipato nelle pagine precedenti, le novità introdotte dallo EHDS per bilanciare le prerogative delle persone fisiche con quelle dei titolari dei dati e degli utenti dovrebbero consentire di evitare l'adozione dell'approccio interpretativo affermatosi in riferimento al GDPR anche nella lettura dello EHDS, il quale deve rispettare – occorre ribadirlo – l'*acquis* europeo per la protezione dei dati personali. Inoltre, il mutato contesto normativo, volto ad agevolare l'uso primario e secondario dei dati, non solo in ambito sanitario, affinché i singoli e la collettività possano trarre beneficio dallo sfruttamento economico e sociale degli stessi, impone una riflessione sul modo in cui il GDPR è stato interpretato finora. In particolare, riteniamo necessario sviluppare alcune ipotesi interpretative alternative del GDPR per assicurare una maggiore coerenza nell'ordinamento giuridico dell'Unione, ma anche per realizzare appieno i "veri" obiettivi del GDPR, sui quali occorre preliminarmente interrogarsi.

Affrontare questo tema è tutt'altro che semplice. Come evidenziato dalla dottrina, infatti, gli interventi legislativi in materia di protezione dei dati sono noti per la loro mancanza di chiarezza in relazione alle finalità perseguite [210], e il GDPR non fa eccezione. Il suo art. 1, rubricato "oggetto e obiettivi", afferma che il regolamento: i) stabilisce norme relative sia alla protezione dei dati personali sia alla libera circolazione di tali dati [211]; ii) mira a tutelare "i diritti e le libertà fondamentali delle persone fisiche, *in particolare* il diritto alla protezione dei dati personali" [212]. Viene inoltre specificato che le ragioni relative alla protezione delle persone fisiche con riferimento al trattamento dei dati personali non devono costituire un limite o un divieto alla libera circolazione dei dati personali nell'Unione [213].

Sebbene il GDPR venga spesso descritto come una normativa finalizzata alla tutela della privacy o del diritto fondamentale alla protezione dei dati

---

[210] Cfr. G. GONZÁLEZ FUSTER, S. GUTWIRTH, *Opening up Personal Data Protection: A Conceptual Controversy*, in *Comput. Law Secur. Rev.*, 2013, vol. 29, p. 531; N. PURTOVA, *Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table…and Back on Again?*, in *Comput. Law Secur. Rev.*, 2014(a), vol. 30, n. 1, pp. 6-23; L.A. BYGRAVE, *Data Privacy Law: An International Perspective*, OUP, Oxford, 2014. Sull'evoluzione della disciplina sulla protezione dei dati in generale, si rinvia a C.J. BENNETT, *Regulating Privacy – Data Protection and Public Policy in Europe and the United States*, Cornell University Press, New York, 1992; V. MAYER SCHÖNBERG, *Generational Development of Data protection in Europe*, in P.E. AGREE., M. ROTENBERG (eds.), *Technology and Privacy: The New Landscape*, The MIT Press, New York, 1997, pp. 219-242.

[211] Art. 1, par. 1, GDPR.

[212] Art. 1, par. 2, GDPR (corsivo aggiunto).

[213] Art. 1, par. 3, GDPR.

personali, nulla nell'articolo preposto a definirne il contenuto e le finalità conferma questa interpretazione. Il primo paragrafo, richiamando quanto disposto dall'art. 16, par. 2, TFUE, stabilisce che il GDPR non si limita a fissare norme sulla protezione dei dati personali, ma anche norme sulla libera circolazione degli stessi. Il paragrafo successivo [214], invece, individua, seppur in modo non del tutto chiaro, gli obiettivi precipui a cui tali norme devono tendere: i) proteggere i diritti e le libertà delle persone fisiche dai danni derivanti dal trattamento dei dati personali e ii) riconoscere l'importanza di attività di trattamento legittime per la società moderna [215], facendo altresì in modo che la "libera circolazione dei dati personali" all'interno dell'Unione non sia né vietata né limitata [216].

Per quanto riguarda il primo obiettivo, è rilevante notare che, diversamente dall'art. 1, par. 1, DPD, il GDPR non menziona esplicitamente il diritto alla vita privata tra i diritti da tutelare. Forte della nuova base giuridica (art. 16,

---

[214] In giurisprudenza, il secondo paragrafo dell'art. 1 GDPR viene spesso letto in combinato disposto ai considerando 10, 11 e 13. Cfr. le sentenze della Corte del 3 aprile 2025, causa C-710/23, *Ministerstvo zdravotnictví (Dati riguardanti il rappresentante di una persona giuridica)*, EU:C:2025:231, punto 29; del 9 gennaio 2025, causa C-394/23, *Mousse*, EU:C:2025:2, punto 21; del 4 ottobre 2024, causa C-446/21, *Schrems (Comunicazione di dati al grande pubblico)*, EU:C:2024:834, punto 45; sentenza *Meta Platforms Ireland (Action représentative)*, punto 48; sentenza *IAB Europe*, punto 53, *Pankki S*, punto 55; sentenza del 4 maggio 2023, causa C-60/22, *Bundesrepublik Deutschland (Casella di posta elettronica degli uffici giudiziari)*, EU:C:2023:373, punto 64; sentenza del 9 febbraio 2023, *X-FAB Dresden*, C-453/20, EU:C:2023:79, punto 25; sentenza *Osterreichische Datenschutzbehörde e CRIF*, punto 40; sentenza del 1°agosto 2022, causa C-184/20, *Vyriausioji tarnybinės etikos komisija*, EU:C:2022:601, punto 125; sentenza *Google LLC*, punto 54; sentenza *Facebook Ireland*, punto 45. Spesso, il riferimento è al solo considerando 10 (sentenze *UI c. Österreichische Post AG*, punto 48; *RW c. Österreichische Post*, punto 44; *Schrems II*, punto 101), mentre, con riferimento alla DPD, i giudici erano soliti richiamare l'art. 1 e i considerando 2 e 3 (sentenze *Rijkeboer*, punto 47, *Satakunnan Markkinapörssi e Satamedia*, punto 52, *Promusicae*, punto 63, *Lindqvist*, punti 97 e 99, e *Österreichischer Rundfunk e a*., punto 70.

[215] P. DE HERT, S. GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in S. GUTWIRTH et al. (eds.), *op. cit.*, 2009, pp. 3-44; P. DE HERT, S. GUTWIRTH, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power*, in *Direito público*, 2022, vol. 18, p. 518.

[216] Art. 1, par. 3, GDPR. Una disposizione analoga all'art. 1, par. 3, GDPR, si trova anche all'art. 1, par. 2, lett. a), direttiva (UE) 2016/680, secondo cui gli Stati membri devono garantire "che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione, qualora tale scambio sia richiesto dal diritto dell'Unione o da quello dello Stato membro, non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali". Questa affermazione viene ribadita riguardo ai trattamenti aventi ad oggetto categorie particolari di dati. Secondo il considerando 53 GDPR, la possibilità per gli Stati membri di introdurre o mantenere, ai sensi dell'art. 9, par. 4, GDPR, ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, biometrici o relativi alla salute, non deve ostacolare la libera circolazione dei dati personali.

par. 2, TFUE) e della vincolatività della Carta [217] che distingue tra i diritti previsti agli artt. 7 e 8 [218], il legislatore europeo sembra voler spezzare il legame tra il diritto alla privacy e il diritto alla protezione dei dati personali [219], abbandonando così l'idea che la protezione dei dati personali debba essere concepita unicamente quale appendice del diritto alla riservatezza e alla dignità umana [220].

In questa prospettiva, i diritti degli interessati (ad es. il diritto di accesso ai dati), espressione del diritto individuale alla protezione dei dati personali, dovrebbero essere intesi non tanto come diritti che conferiscono agli interessati

---

[217] Art. 6, par. 1, TUE. Sulle conseguenze derivanti dall'acquisizione di valore vincolante delle disposizioni della Carta, v. G. STROZZI, *Il sistema integrato di tutela dei diritti fondamentali dopo Lisbona: attualità e prospettive*, in L.F. PACE (a cura di), *Nuove tendenze del diritto dell'Unione europea dopo il Trattato di Lisbona*, Giuffrè, Milano, 2012, p. 34 ss.; G. DE BÙRCA, *After the Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?*, in *MJECL*, 2013, vol. 20, n. 2, pp. 168-184; W. WEIß, *The Human Rights Regime Post Lisbon: Turning the CJEU into a Human Rights Court*, in S. MORANO-FOADI, L. VICKERS (eds.), *Fundamental Rights in the EU: A Matter for Two Courts*, Hart Publishing, Oxford-Portland, 2015, pp. 69-88; G. DI FEDERICO, *Fundamental Rights in the EU: Legal Pluralism and Multi-Level Protection After the Lisbon Treaty*, in G. DI FEDERICO (ed.), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*, Springer, Dordrecht, 2011, p. 38; L. DANIELE, *La protezione dei diritti dell'uomo nell'Unione europea dopo il Trattato di Lisbona*, in *DUE*, 2009, vol. 3, p. 652; M. CARTABIA, *L'impatto costituzionale della Carta dei diritti fondamentali dell'Unione europea*, in M. CARTABIA (a cura di), *Liber amicum Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, 2018, p. 183.

[218] Sul tema si rinvia anche a G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Cham, 2014; M. TZANOU, *Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right*, in *Int. Data Priv. Law*, 2013, vol. 3, n. 2, pp. 88-99; O. LYNSKEY, *op. cit*., 2014, pp. 569-597; P. HUSTINX, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, in M. CREMONA (ed.), *New Technologies and EU Law*, OUP, Oxford, 2017, pp. 123-173; J. KOKOTT, C. SOBOTTA, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *Int. Data Priv. Law*, 2013, vol. 3, pp. 222-228; R. GELLERT, S. GUTWIRTH, *The Legal Construction of Privacy and Data Protection*, in *Comput. Law Secur. Rev.*, 2013, vol. 29, pp. 522-530.

[219] Anche a livello terminologico, diverse scelte compiute dal legislatore del GDPR vanno in questa direzione. Ad esempio, non si parla più di "*privacy by design*", bensì di protezione dei dati sin dalla progettazione (art. 25 GDPR), oppure alla "valutazione di impatto sulla privacy", viene preferita la dicitura "valutazione dell'impatto sulla protezione dei dati" (art. 35 GDPR).

[220] L. COSTA, Y. POULLET, *Privacy and the Regulation of 2012*, in *Comput. Law Secur. Rev.*, 2012, vol. 28, p. 255, dove si sottolinea come questa separazione tra il diritto alla protezione dei dati personali e il diritto alla privacy "*cuts the Data Protection regulation from the innovative and quite protective Strasbourg Court's jurisprudence which repeats that privacy might be considered as the way to achieve the right to self-determination, to dignity and, to that extent, represents an essential condition for all liberties*". Per ulteriori riferimenti dottrinali sul punto, si rimanda alla sezione 4.2 del capitolo 2 e, in particolare, alla nota 178.

il "dominio" sui propri dati, escludendo altri dal loro utilizzo, quanto piuttosto come diritti individuali di controllo [221], che assicurano l'esercizio di poteri di supervisione e anche di intervento rispetto alle attività di trattamento [222]. Tra i diritti previsti dal GDPR, infatti, ve ne sono alcuni finalizzati a consentire agli interessati di esercitare un controllo sulla liceità del trattamento (ad es. il diritto a ricevere informazioni sul trattamento e a ottenere l'accesso ai dati) [223], e altri volti a permettere loro di esercitare un controllo "proattivo" non solo sul trattamento (ad es. il diritto ad autorizzare il trattamento) [224], ma anche sui dati stessi (ad es. il diritto di modificare e cancellare i dati) [225].

Tali diritti dovrebbero quindi essere interpretati non come diritti di esclusiva sui dati [226], bensì come strumenti di *empowerment* per gli individui che

---

[221] In questo senso, v. le conclusioni dell'Avvocato generale Campos Sánchez-Bordona in *UI c. Österreichische Post AG*, punti 70-71 e 75. La riflessione dell'Avvocato generale sull'esistenza nel GDPR del "controllo" come valore o obiettivo indipendente della normativa viene sviluppata in risposta all'argomentazione addotta dalle parti relativa all'esistenza di una presunzione incontestabile di danno qualora una violazione del GDPR comporti una "perdita di controllo". Secondo l'Avvocato generale, questo tipo di presunzione è da escludere, in quanto la perdita di controllo non determina necessariamente l'insorgere di un danno (punto 62). In dottrina, il concetto di controllo presente nella disciplina della protezione dei dati è stato equiparato a una sorta di "*toolbox at the disposal of the data subjects: they get equipped with a set of 'micro-rights' which supposedly enable them to be in control at the different stages of the processing of their data*" (C. LAZARO, D. LE MÉTAYER, *Control Over Personal Data: True Remedy or Fairy Tale?*, in *SCRIT-ed*, 2015, vol. 12, n. 1, p. 15).

[222] Per una classificazione alternativa dei diritti contenuti nel GDPR, si rinvia a L. CALIFANO et al., *op. cit.*, 2023, p. 224. Gli A. distinguono tra i diritti conoscitivi (ad es. il diritto all'informazione e all'accesso) e i diritti di controllo sui dati (ad es. il diritto di rettifica, di cancellazione e di portabilità) e sul trattamento (ad es. il diritto di opposizione e di limitazione), nonché tra diritti a contenuto positivo, che impongono un obbligo di eseguire un'attività specifica (ad es. la rettifica e la cancellazione) e i diritti a contenuto negativo, che richiedono al soggetto passivo si astenersi da un'attività (ad es. il diritto di opposizione).

[223] Rispettivamente, artt. 13-14 e 15 GDPR. A questi si aggiunge il diritto di ricevere informazioni su specifici destinatari a cui sono state comunicate rettifiche, cancellazioni, limitazioni del trattamento (art. 19) e su gravi anomalie incorse nel trattamento (art. 34).

[224] Artt. 6, par. 1, lett. a) e 9, par. 2, lett. a), GDPR. Oltre al consenso, hanno la medesima funzione anche i diritti di limitazione (art. 18), di revoca del consenso (art. 7, par. 3), di opposizione al trattamento (art. 21) e di non essere sottoposti a un trattamento unicamente automatizzato (art. 22).

[225] Rispettivamente, artt. 16-17 GDPR. Si pensi anche al diritto alla portabilità (art. 20) che, diversamente dal diritto di accesso, non ha una natura puramente informativa, ma assume una natura dinamica, attribuendo alla persona un ruolo attivo nella tutela del proprio diritto alla protezione dei dati personali. Cfr. S. RODOTÀ, *Tecnologie e diritti*, Il Mulino, Bologna, 2021, p. 70 ss.

[226] Su questo aspetto, tuttavia, la dottrina non è unanime. Alcuni autori hanno ravvisato nei diritti presenti nel GDPR (ad es. il diritto alla cancellazione) una volontà legislativa di instaurare un regime proprietario in questa materia (S.C. BENNET, *Right to Be Forgotten:*

permettono loro "*to participate in, and have a measure of influence over, the processing of data on them by other individuals or organizations*" [227]. A ciò si aggiunge che, alla stregua del diritto alla protezione dei dati personali, questi diritti non sono assoluti [228]. Oltre alle specifiche limitazioni che possono essere introdotte a livello nazionale *ex* art. 23 GDPR, sono previste ulteriori ipotesi derogatorie. Ad esempio, limiti ai diritti individuali si hanno in caso di trattamenti a fini giornalistici [229] e per scopi di archiviazione nell'interesse pubblico o ricerca scientifica [230], nonché con riferimento al diritto alla portabilità [231].

Passando al secondo obiettivo, vale la pena di sottolineare che l'impianto normativo del GDPR non si limita a concedere diritti agli interessati, ma stabilisce anche le regole che consentono di svolgere in modo legittimo le attività di trattamento dei dati personali [232]. Come ricordato dalla stessa Commissione nella Comunicazione di accompagnamento alla proposta del GDPR, l'elevato livello di protezione dei dati personali è strumentale all'accrescimento della fiducia nei servizi online – requisito necessario per sfruttare il potenziale dell'economia digitale e promuovere "la crescita e la competitività delle industrie europee" [233]. Le tutele riconosciute agli interessati, tramite l'attribuzione di diritti individuali e l'imposizione di obblighi ai titolari del trattamento

---

Reconciling EU and US Perspectives, in *Berkeley J. Int. L*, 2012, vol. 30, p. 161, D. ZWICK, N. DHOLAKIA, *Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right*, in *Electronic Markets*, 2001, vol. 11, p. 116). Altri, invece, sostengono che né la DPD né il GDPR introducono diritti di esclusiva per gli interessati e/o i titolari (N. PURTOVA, *The Illusion of Personal Data as no One's Property*, in *Law, Innov. Technol.*, 2015, vol. 7, n. 1, p. 93 ss).

[227] L.A. BYGRAVE, *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, The Hague, 2002.

[228] Nel commentare la proposta del GDPR, N. PURTOVA, *op. cit*., 2014(a), p. 17 già nel 2014 criticava il fatto che i diritti alla cancellazione, opposizione e portabilità dei dati personali, specialmente nel caso di attività di trattamento che non si fondano sul consenso, finissero per essere piuttosto limitati.

[229] Art. 85, par. 2, GDPR.

[230] Art. 89, parr. 2-3, GDPR. Si vedano, altresì, le deroghe previste dagli artt. 14, par. 5, lett. b), art. 17, par. 3, lett. d) e 21, par. 6), GDPR

[231] Art. 20 GDPR. Questo opera solo in caso di trattamenti automatizzati fondati sul consenso o su un contratto (par. 1). Inoltre, la trasmissione dei dati personali da un titolare all'altro deve essere tecnicamente fattibile (par. 3) e non deve ledere i diritti e le libertà altrui (par. 4).

[232] G. COMANDÉ, *Ricerca in sanità e data protection un puzzle…risolvibile*, in *Rivista italiana di medicina legale*, 2019(b), fasc. 1, p. 192 in cui si osserva come il "cambiamento di enfasi dalla *privacy* alla protezione dei dati si riflette su tutto il Regolamento".

[233] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo, COM(2012) 9 final, del 25 gennaio 2012, punto 1.

(*in primis*, il rispetto dei principi di cui all'art. 5 GDPR), non sono pensate per frenare il trattamento dei dati, bensì per favorirlo, in modo che la società intera ne possa trarre beneficio.

Il rapporto di strumentalità del trattamento di dati personali per il pieno conseguimento del "benessere delle persone" è evidente nel considerando 4 GDPR, dove si afferma che il "trattamento dei dati personali dovrebbe essere al servizio dell'uomo" [234], contribuendo "alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche" [235]. Di estrazione giurisprudenziale [236], questo considerando richiama l'art. 52 della Carta [237] e recupera l'accezione di diritto alla protezione dei dati elaborata dalla dottrina tedesca e, successivamente, fatta propria dal Tribunale costituzionale tedesco nella sentenza sul Censimento (*Volkszählungsurteil*), in cui viene fatto esplicito riferimento al concetto di "autodeterminazione informativa" (*informationelle Selbstbestimmung*) [238].

---

[234] Considerando 4 GDPR. Si noti come, per esplicita volontà del Consiglio, tale disposizione è stata inserita tra i primi considerando, rispetto invece alla posizione iniziale scelta dalla Commissione, ossia il considerando 139 (COD, 11326/12, fn 6). La dimensione "collettiva" delle norme sulla protezione dei dati è particolarmente forte nel diritto nazionale tedesco in cui si afferma che "*self-determination is an essential prerequisite for a free and democratic society that is based on the capacity and solidarity of its citizens*" (BVerfG, Ordinanza del Primo Senato del 15 dicembre 1983 – 1 BvR 209/83, punto 146) e in quello francese, per cui "*informatics must be at the service of each citizen. […] It may not endanger human identity, human rights, private life, or individual or public liberties*" (art. 1 *loi 78-17/78 relative à l'informatique, aux fichiers et aux libertés*).

[235] Considerando 2 GDPR.

[236] Sentenze *Vyriausioji tarnybinės etikos komisija*, punto 52, *Google (Ricerca di contenuti presumibilmente inesatti)*, punto 56 e *GC e a*., punto 58, *Google LLC*, punto 60; parere della Corte n. 1/15; sentenze *Tele2 Sverige*, punti 96 e 103, *Schrems I*, punto 92, *Digital Rights Ireland*, punto 52; sentenze del 22 gennaio 2013, causa C-283/2011, *Sky Österreich GmbH c. Österreichischer Rundfunk*, ECLI:EU:C:2013:28, punto 45; del 6 settembre 2012, causa C-544/10, *Deutsches Weintor*, ECLI:EU:C:2012:526, punto 54; del 9 settembre 2004, cause riunite C-184/02 e C-223/02, *Spagna e Finlandia/Parlamento e Consiglio*, ECLI:EU:C:2004:497, punti 51 e 52; sentenza *Satakunnan Markkinapörssi e Satamedia*, punto 56; sentenza del 13 luglio 1989, causa C-5/88, *Wachauf c. Repubblica federale di Germania*, ECLI:EU:C:1989:321, punto 17.

[237] T. GROPPI, *Comm. all'art. 52*, in R. BIFULCO, M. CARTABIA, A. CELOTTO, *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, il Mulino, Bologna, 2001, p. 351 ss., in cui viene sottolineata la natura di "clausola limitativa generale" dell'art. 52 della Carta che la rende applicabile "a tutti i diritti e le libertà garantiti dalla Carta. Non ci sono, quindi, diritti il cui esercizio non possa essere sottoposto a limiti, ma le limitazioni debbono avvenire entro il quadro di principi delineato da tale disposizione".

[238] Per un commento sulla sentenza, cfr. G. SARTOR, *Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del*

In questa occasione, i giudici tedeschi hanno affermato che, sebbene "il libero sviluppo della personalità umana, nel moderno contesto del trattamento dei dati, presuppone la tutela dei singoli contro la raccolta, memorizzazione, utilizzazione e trasferimento senza limitazioni dei suoi dati personali", "l'informazione, anche se è relativa ad una persona, mostra un'immagine della realtà sociale che non può essere nell'esclusiva disponibilità degli interessati. La Costituzione […] ha risolto la tensione individuo-comunità nel senso di un adattamento e di un assoggettamento della persona alla comunità. Il singolo individuo deve perciò accettare limitazioni del suo diritto all'autodeterminazione informativa nel caso in cui vi siano interessi generali preminenti" [239]. In altre parole, dunque, pur riconoscendo che il diritto all'autodeterminazione informativa conferisce all'individuo un potere dispositivo sui propri dati, il Tribunale costituzionale tedesco ha precisato che tale diritto non può assumere i connotati dell'assolutezza tipici dei regimi proprietari, dal momento che l'uso e la circolazione dei dati costituiscono elementi indispensabili per la collettività.

Se si utilizza questa chiave di lettura per interpretare il GDPR, ne consegue che i suoi obiettivi non dovrebbero essere intesi nel senso di "ampliare il controllo del singolo sulle informazioni che lo riguardano, semplicemente assecondandone le preferenze, bensì [di] conciliare il diritto alla protezione dei dati personali con gli interessi dei terzi e della società" [240]. Non dissimile d'altronde è la visione dei primi commentatori del GDPR, che lo hanno considerato come una normativa molto più attenta al valore economico dei *Big Data* e al potenziale derivante dalla loro libera circolazione, piuttosto che al diritto individuale alla protezione dei dati personali [241].

1983 nel dibattito dottrinale sui profili costituzionalistici del "Datenschutz", in *Informatica e Diritto*, 1986, vol. 12, p. 95 ss.

[239] Corte suprema tedesca del 15 dicembre 1983, BvR 209/83, BVerfGE 65. Il caso in questione riguarda la legittimità costituzionale di una legge federale concernente il censimento dei cittadini tedeschi, compiuto per avere cognizione della situazione socioeconomica della popolazione. In seguito all'opposizione di cittadini che lamentavano la raccolta di un numero eccessivo di dati e la mancanza di limiti circa un loro successivo utilizzo da parte di enti amministrativi, i giudici hanno dichiarato la parziale illegittimità costituzionale della legge. Richiamando il diritto alla personalità previsto dai primi due articoli della Costituzione federale, i giudici tedeschi hanno stabilito che uno dei corollari del diritto alla personalità è rappresentato dalla possibilità di essere informati sull'utilizzo dei propri dati e di intervenire nel caso in cui vi siano violazioni della propria sfera giuridica (punti 143-146).

[240] Conclusioni dell'Avvocato generale Campos Sánchez-Bordona in *UI c. Österreichische Post AG*, punto 81.

[241] A questo proposito, risultano interessanti le osservazioni svolte da Purtova nel commentare l'adozione del GDPR: "*the proposed Regulation effectively puts the possibility of having informational self-determination as a normative cornerstone of data protection off the table, or, at the minimum, reduces the meaning of informational self-determination to the point*

Tra questi, Purtova ha evidenziato, ad esempio, che mentre con la DPD si era cercato di raggiungere un equilibrio tra i diritti e gli interessi coinvolti insistendo sugli aspetti procedurali [242], con la proposta di GDPR si è assistito a un ridimensionamento dei "*default control rights of an individual over his/her personal data*" (ad es. rendendo più difficile l'esercizio del consenso tramite l'introduzione di condizioni specifiche) e a un contestuale ampliamento dell'ambito di applicazione dei "*rights of others in personal data*" [243]. In particolare, si afferma che "*[t]he degree to which the Regulation accommodates the interests of others is so significant that the Regulation's rules of data processing effectively shift the balance away from the informational self-determination and default individual's entitlement in favour of competing (business) interests and the default entitlement of others to process*", intervenendo sui limiti al controllo degli individui già presenti nella DPD [244].

A dieci anni dall'adozione del GDPR, ci si domanda che fine abbiano fatto i "*rights of others in personal data*" nell'interpretazione di questa disciplina. Forse per evitare una regressione nella tutela degli interessati, la giurisprudenza della Corte ha finito per eccedere nel senso opposto, sacrificando i diritti e gli interessi che soggetti terzi possono legittimamente avere nel trattamento dei dati personali. A partire da questo quadro, cercheremo di delineare alcune ipotesi interpretative delle norme del GDPR che riteniamo possano meglio riflettere gli obiettivi originari di tale disciplina. A questo proposito, ci concentreremo sulle disposizioni del GDPR che, nella sezione 2, abbiamo

---

of no significance. The proposed Regulation signifies the choice in favour of the Information Industry's default entitlement to collect and further process personal data as a normative foundation and a rationale of data protection in Europe. The LIBE Compromise text corrects the most controversial of the Commission's original choices in favour of the individual's default entitlements, not installing, but certainly putting the Informational self-determination as a possible rationale of the European data protection back on the negotiation table" (N. PURTOVA, *op. cit.*, 2014(a), p. 6).

[242] N. PURTOVA, *op. cit*., 2014(a), p. 7 richiama sul punto le considerazioni effettuate da L.A. BYGRAVE, *op. cit*., 2002, p. 84: "*[t]he predominance of procedural concerns appears symptomatic of legislators' uncertainty about the nature of the interests to be protected, together with a desire for regulatory flexibility in the face of technological complexity and change*". Sulle difficoltà nella negoziazione del testo finale della DPD, derivante dalla necessità di conciliare visioni nazionali differenti sul diritto alla protezione dei dati personali, si rimanda a D. HEISENBERG, *Negotiating Privacy: The European Union, The United States, and Personal Data Protection*, Lynne Rienner Pub, Boulder, 2005.

[243] N. PURTOVA, *op. cit*., 2014(a), p. 9. Di recente, è stato messo in luce come l'attenuarsi dell'approccio di forte tutela delle prerogative individuali, a favore di un maggiore riconoscimento degli interessi a trattare i dati, è stato il frutto delle modifiche proposte dal Consiglio. Al contrario, gli emendamenti del Parlamento puntavano a rendere la proposta della Commissione "*much more oriented towards individual rights*" (J. HILDEN, *Lobby in/Policy out? Assessing Lobbyist Influence on the GDPR*, in *Eur. Data Prot. L. Rev.*, 2021, vol. 7, p. 531).

[244] N. PURTOVA, *op. cit*., 2014(a), p. 17.

individuato come potenzialmente più problematiche, ossia quelle relative al campo di applicazione *ratione materiae* della disciplina (sezione 3.2.1) e quelle che consentono di bilanciare il diritto alla protezione dei dati con altri diritti e libertà fondamentali (sezione 3.2.2).

3.2.1. I limiti all'ambito di applicazione materiale

In tempi non sospetti, Purtova prevedeva che la legge sulla protezione dei dati personali sarebbe potuta diventare "*the law of everything*" [245]. Oggi, possiamo affermare senza timore di smentite che questa previsione si è avverata. L'interpretazione estensiva di concetti chiave (ad es. il trattamento e i dati personali), combinata a un'interpretazione restrittiva delle eccezioni all'ambito di applicazione materiale della disciplina europea sui dati personali [246], ha reso il suo campo di applicazione sostanzialmente illimitato [247]. Particolarmente pregnante a questo proposito è un passaggio delle conclusioni dell'Avvocato generale Bobek in una causa relativa alla possibilità per i giornalisti, nei Paesi Bassi, di accedere ad atti giudiziari al fine di offrire informazioni corrette alla collettività:

"Se una sera vado in un locale e condivido con quattro miei amici intorno a un tavolo in un luogo pubblico [che dunque probabilmente non soddisfa l'eccezione per l'esercizio di attività personali o domestiche …] un'osservazione piuttosto poco lusinghiera sul mio vicino contenente i suoi dati personali, che ho appena ricevuto via e-mail (quindi in modo automatizzato e/o facente parte del mio archivio), divento forse io il responsabile del trattamento di questi dati e improvvisamente soggetto a tutti gli obblighi (piuttosto gravosi) del GDPR? Poiché il mio vicino non ha mai fornito il consenso a tale trattamento (comunicazione mediante trasmissione), e poiché è alquanto improbabile che il pettegolezzo figuri tra i motivi legittimi elencati nell'articolo 6 del GDPR, con tale comunicazione incorro nella violazione di una serie di disposizioni del GDPR, compresa la maggior parte dei diritti dell'interessato" [248].

---

[245] N. PURTOVA, *op. cit.*, 2018, pp. 40-81,

[246] Si veda, in particolare, la giurisprudenza analizzata nella sezione 2.1 del presente capitolo.

[247] Cfr. le conclusioni dell'Avvocato generale Bobek in *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali*, punto 1, dove si afferma che il GDPR "non è un atto normativo di portata limitata. Il suo ambito di applicazione definito in maniera ampia, il fatto che qualsiasi eccezione a quest'ultimo sia stata svuotata della sua sostanza dalla giurisprudenza, nonché l'approccio alla sua interpretazione basato sulle definizioni, astratto e di conseguenza piuttosto vasto, hanno contribuito a rendere l'ambito di applicazione del GDPR praticamente illimitato. Infatti, adottando un siffatto approccio, è piuttosto difficile al giorno d'oggi trovare una situazione in cui qualcuno non stia trattando dati personali da qualche parte in qualche momento".

[248] Conclusioni dell'Avvocato generale Bobek del 6 ottobre 2021, causa C-245/20,

Questo episodio fittizio, creato ad arte dall'Avvocato generale, dimostra come l'assenza di limiti sostanziali al campo di applicazione del GDPR e le interpretazioni estensive della Corte stiano contribuendo a trasformarlo "in una delle normative del diritto dell'Unione di fatto più disattese" [249]. Infatti, la maggior parte delle persone potrebbe non essere consapevole dell'obbligo di conformarsi agli standard di protezione stabiliti nel GDPR. Tuttavia, sebbene ciò possa essere vero per i *laymen*, ai quali l'Avvocato generale Bobek fa riferimento nell'esempio della conversazione tra amici in un locale, la situazione cambia per coloro che conoscono il GDPR e le conseguenze sanzionatorie che possono derivare dalla sua violazione.

In questi casi, come abbiamo già sottolineato, la sostanziale assenza di limiti all'ambito di applicazione materiale del GDPR può rendere difficile comprendere quali siano i confini tra il medesimo e altre normative che disciplinano attività di trattamento di dati, compresi quelli personali, come il DGA, il DA e lo EHDS. Inoltre, l'ampia portata del GDPR può spingere i titolari del trattamento a adottare comportamenti "difensivi", che consistono nella rinuncia a utilizzare i dati per evitare di dover adempiere ai numerosi obblighi

---

Autoriteit Persoonsgegevens, ECLI:EU:C:2021:822, punto 56. Un'operazione simile era stata compiuta dall'Avvocato generale Jääskinen, nelle conclusioni del 25 giugno 2013 in *Google Spain*, punto 29: "Si pensi ad un professore di diritto europeo che abbia scaricato sul suo portatile la giurisprudenza essenziale della Corte dal sito della stessa. A termini della direttiva, questo professore potrebbe essere considerato un 'responsabile del trattamento' di dati personali provenienti da un soggetto terzo. Il professore è in possesso di file contenenti dati personali trattati automaticamente a scopo di ricerca e di consultazione nell'ambito di attività che non sono puramente personali o domestiche. In realtà, chiunque oggi legga un giornale su un tablet o segua un social media su uno smartphone apparentemente effettua un trattamento di dati personali tramite strumenti automatizzati e potrebbe teoricamente rientrare nell'ambito di applicazione della direttiva nella misura in cui tale attività si svolga al di fuori della sua stretta sfera privata".

[249] *Ibid.* punto 65. In dottrina è stato inoltre evidenziato che l'eccesso di applicazione del GDPR può generare due fenomeni che rischiano di svilire o addirittura ridicolizzare tale disciplina. Il primo riguarda il ricorso da parte dei titolari del trattamento di "surrogati di conformità" (ad es. schemi di certificazione) (N. PURTOVA, *op. cit*., 2018, p. 77), spesso forniti da soggetti privati con forti interessi commerciali (N. PURTOVA, *Who Decides on the Future of Data Protection? Role of Law Firms in Shaping European Data Protection Regime*, in *Int. Rev. Law Comput.*, 2014(b), vol. 28, n. 2, p. 204) e che non richiedono al titolare un'effettiva valutazione della correttezza delle proprie attività, ma forniscono una mera parvenza di conformità formale al GDPR. Il secondo fenomeno consiste nel c.d. "*selective enforcement*", secondo il quale le autorità di controllo, impossibilitate nel loro compito di monitorare il rispetto di una normativa dall'ampia portata, si limitano a verificare la conformità solo di alcune norme, individuate attraverso "*priority lists and shortcuts*" (N. PURTOVA, *op. cit*., 2018, p. 77. Problematiche connesse all'*enforcement* sono state sottolineate anche di recente in un'analisi relativa all'estensione dell'applicabilità del GDPR ai *code*, v. N. PURTOVA, R. LEENES, *Code as Personal Data: Implications for Data Protection Law and Regulation of Algorithms*, in *Int. Data Priv. Law*, 2023, vol. 13, n. 4, pp. 245-266).

previsti da questa normativa. Tali comportamenti rischiano, specialmente in ambito sanitario, di limitare *ab origine* le opportunità di crescita economica e sociale dell'Unione.

Pertanto, per evitare conseguenze pratico-giuridiche irrazionali, l'ambito di applicazione della disciplina europea sulla protezione dei dati personali non dovrebbe essere esteso "oltre misura" [250]. A questo proposito, sebbene nel testo del GDPR siano stati utilizzati termini generici per definire concetti chiave come "trattamento" e "dati personali" (ad es. "qualsiasi" [251] o "rivelano" [252]), una delimitazione del suo ambito di applicazione *ratione materiae* sembra ancora possibile.

Per quanto riguarda il concetto di "trattamento", abbiamo osservato in precedenza che, per essere esclusi ai sensi dell'art. 2, par. 1, GDPR, i trattamenti devono essere manuali, non strutturati, né destinati a diventare strutturati o automatizzati, e non devono essere combinati nemmeno in parte con un trattamento automatizzato [253]. Nel caso in cui i trattamenti fossero manuali ma strutturati, ossia organizzati secondo criteri determinati all'interno di un archivio, dovrebbero rientrare nell'ambito di applicazione del GDPR. Di conseguenza, la nozione di "archivio" diventa dirimente. Sebbene la Corte ne abbia fornito un'interpretazione estensiva, giustificata dalle scelte lessicali compiute dal legislatore e dal principio di neutralità degli strumenti utilizzati per il trattamento [254], al fine di evitare letture troppo ampie, si dovrebbe porre maggiore enfasi sul requisito secondo il quale i dati raccolti durante le attività di trattamento, oltre a essere contenuti in un archivio, devono essere strutturati sulla base di criteri specifici (ad es. i dati sono connessi tra loro per contenuto o finalità) [255].

Inoltre, pur rispettando il principio secondo cui un'eccezione deve essere interpretata restrittivamente, sarebbe opportuno chiarire alcune delle ipotesi derogatorie all'ambito di applicazione contenute nell'art. 2, par. 2, GDPR. Ad

---

[250] Parere del WP n. 04/2007, p. 4. Sebbene il riferimento sia alla DPD, l'analisi svolta dal WP può essere estesa anche al GDPR, dal momento che questo non va a modificare la nozione contenuta nella DPD.

[251] Art. 4, n. 1 (dato personale), 2 (trattamento) e 6 (archivio) GDPR.

[252] Art. 4, n. 15 e considerando 35 (dati relativi alla salute), ma anche art. 9, par. 1 (dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale) GDPR.

[253] Vedi anche considerando 15 GDPR.

[254] Sentenze *Edemol*, punti 34 e 37 e *Jehovan todistajat*, punti 53 e 56-58.

[255] Considerando 15. La Corte ha riservato maggiore attenzione a questo aspetto nella sentenza *Jehovan todistajat*, specificando tuttavia che "il requisito secondo cui l'insieme di dati personali deve avere un carattere 'strutturato secondo criteri specifici' mira *unicamente* a consentire che i dati relativi a una persona possano essere individuati facilmente" (punto 57 – corsivo aggiunto).

esempio, riguardo all'art. 2, par. 2, lett. a), GDPR ("attività che non rientrano nell'ambito di applicazione del diritto dell'Unione"), i criteri per distinguere tra le attività relative alla sicurezza nazionale, volte a tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società, e le attività proprie dello Stato o di un'autorità dovrebbero essere identificati con maggiore precisione.

Secondo una consolidata giurisprudenza della Corte, solo le prime sono escluse dal campo di applicazione materiale del GDPR [256], mentre le seconde potrebbero rientrarvi [257]. Attualmente, l'unico criterio fornito dalla Corte per stabilire che un'attività di trattamento non è soggetta al GDPR non è tanto l'identità dell'autore del trattamento, quanto piuttosto la natura dell'attività svolta [258], la quale deve avere per oggetto *immediato* la sicurezza nazionale [259], mentre non è sufficiente un contributo *indiretto* alla salvaguardia della sicurezza nazionale [260]. Un criterio di questo tipo lascia all'interprete un margine di apprezzamento tale da poter giustificare, in futuro, decisioni che, anziché ridimensionare il campo di applicazione del GDPR, possono estenderlo ulteriormente.

Lo stesso vale per i criteri stabiliti con riferimento all'eccezione domestica (o "*household exception*") di cui all'art. 2, par. 2, lett. c), GDPR, e in particolare il criterio del contesto pubblico in cui avviene il trattamento. A differenza di quello dell'ambito di circolazione impressa ai dati [261], il criterio del contesto

---

[256] Cfr. sentenze *Österreichische Datenschutzbehörde c. WK*, punto 46 e *Commissione europea c. Repubblica di Polonia (Indipendenza e privacy dei giudici)*, punto 318; sentenza del 20 ottobre 2022, causa C-306/21, *Koalitsia "Demokratichna Bulgaria – Obedinenie"*, ECLI:EU:C:2022:813, punto 40; sentenza *Latvijas Republikas Saeima (punti di penalità)*, punto 67.

[257] Cfr. sentenze *Österreichische Datenschutzbehörde c. WK* (attività di una commissione parlamentare di inchiesta per il controllo del potere esecutivo), *Koalitsia "Demokratichna Bulgaria – Obedinenie"* (attività relative all'organizzazione di elezioni in uno Stato membro), *Latvijas Republikas Saeima (punti di penalità)* (attività riguardanti la sicurezza stradale), *Land Hessen* (attività di una commissione per le petizioni del Parlamento di uno Stato federato di uno Stato membro), e *Jehovan todistajat* (attività di predicazione porta a porta).

[258] Sentenza *Österreichische Datenschutzbehörde c. WK*, punto 51.

[259] Conclusioni dell'Avvocato generale Szpunar dell'11 maggio 2023, causa C-33/22, *Österreichische Datenschutzbehörde c. WK*, ECLI:EU:C:2023:397, punto 114, sottolinea che la commissione di inchiesta è investita solamente di un compito di controllo nei confronti degli organi del governo federale.

[260] *Ibid.* punto 116. Vedi sul punto anche la sentenza *Land Hessen*, punto 71.

[261] Sulla base di questo criterio, un'attività non rientra nell'eccezione domestica quando si verifica una circolazione indiscriminata di dati, valutata tenendo conto della tenuità del rapporto familiare o amicale, o altre ragioni incompatibili con il concetto di dimensione puramente domestica o familiare. Tale criterio è stato utilizzato nelle sentenze *Buivids* (pubblicazione di un video, senza alcuna restrizione di accesso, su un sito Internet), *Satakunnan*

pubblico amplia notevolmente le possibilità che un trattamento sia soggetto alla disciplina del GDPR. Infatti, ritenere che qualsiasi attività di trattamento che "si estende, anche solo parzialmente, allo spazio pubblico" [262] non può rientrare nell'eccezione domestica, appare andare oltre a quanto previsto *ex lege*. Di conseguenza, sarebbe preferibile, anche se non del tutto risolutivo, utilizzare il criterio della finalità d'uso dei dati [263], secondo il quale un'attività di trattamento dovrebbe considerarsi esclusa dall'ambito di applicazione del GDPR qualora la raccolta, sebbene avvenga in uno spazio non strettamente domestico o personale, sia effettuata per finalità strettamente personali [264].

Passando alla nozione di "dato personale", pare opportuno, da un lato, mettere in discussione i tre criteri individuati dal WP nel parere n. 04/2007 per stabilire quando un dato riguarda una persona fisica e, dall'altro, chiarire il significato del requisito dell'identificabilità. Relativamente al primo aspetto, anziché seguire il test del "contenuto, finalità ed effetto" del WP, sarebbe preferibile interpretare "relativa a" facendo riferimento esclusivamente al contenuto dell'informazione in questione [265], senza estendere l'analisi alla sua

---

Markkinapörssi e Satamedia, punto 44 (accesso a informazioni da parte di un numero illimitato di persone), e *Lindqvist*, punto 47 (pubblicazione di dati personali su un blog di Internet accessibile a un numero indeterminato di persone).

[262] Sentenza *Ryneš*, punto 33 (utilizzo di un sistema di videocamera installata da una persona fisica sulla sua abitazione e in grado di filmare l'ingresso di tale casa, la strada pubblica e l'ingresso della casa situata di fronte).

[263] Parere del WP n. 04/2007.

[264] Benché combinato con quello del contesto pubblico, questo criterio è stato utilizzato in *Jehovan todistajat*, dove la Corte ha affermato che "un'attività non può essere considerata a carattere esclusivamente personale o domestico […] se il suo scopo è quello di rendere i dati personali accessibili a un numero indefinito di persone, ovvero se tale attività si estende, anche solo parzialmente, allo spazio pubblico, e pertanto è diretta verso l'esterno della sfera privata della persona che procede al trattamento dei dati" (punti 42-43). Nel caso di specie, la Corte ha dichiarato che "l'attività di predicazione porta a porta, nel cui ambito i membri della comunità dei testimoni di Geova raccolgono dati personali ha, per sua stessa natura, la finalità di diffondere il credo della comunità dei testimoni di Geova presso persone che […] non appartengono al nucleo familiare dei membri predicatori".

[265] In questo senso, v. la sentenza *YS e Minister voor Immigratie, Integratie en Asiel*, dove i giudici interpretano la nozione di "dato personale" limitandosi a verificare se il contenuto dell'informazione in questione (nel caso di specie, l'analisi giuridica contenuta in una minuta concernente una domanda di permesso di soggiorno) riguardasse la persona fisica. Come evidenziato nella sezione 2 di questo capitolo, tale orientamento non ha trovato seguito nella giurisprudenza successiva: si pensi, *inter alia*, alla sentenza *Nowak* e, più recentemente, alla pronuncia della Corte del 4 settembre 2025, causa C-413/23, *EDPS c. CRU*, ECLI:EU:C:2025:645. In quest'ultima, la Corte – nel confermare la propria giurisprudenza – ha sottolineato che "un esame vertente sul contenuto di un'informazione non deve necessariamente essere completato da un'analisi della finalità e degli effetti di tale informazione, come indica l'impiego della congiunzione 'o' che collega i diversi criteri considerati da tale giurisprudenza" (punto 56).

finalità (ossia quando essa sia destinata a valutare una persona fisica o alcuni suoi aspetti) o al risultato (quando produca effetti apprezzabili sulla sfera dei diritti e delle libertà individuali). In particolare, con riferimento ai dati relativi alla salute, il legame relazionale tra le informazioni e l'interessato non dovrebbe essere interpretato estensivamente facendo riferimento alla capacità dell'informazione di "rivelare" – anche solo indirettamente – dati sullo stato di salute della persona [266].

Per quanto riguarda il secondo aspetto, invece, la soglia per l'identificabilità dovrebbe essere innalzata, affinché un dato che concerne una persona identificabile venga considerato "dato personale" solo dopo un'attenta valutazione in concreto che accerti: i) l'esistenza di informazioni aggiuntive che permettono di re-identificare una persona fisica; ii) la reale possibilità per il destinatario di accedere a queste informazioni [267]. Ne deriva che uno stesso dato può essere qualificato come "personale" per alcuni titolari del trattamento, ma non per altri che non dispongono dei mezzi necessari per ottenere le ulteriori informazioni per identificare nuovamente la persona fisica a cui i dati si riferiscono.

Questa impostazione trova conferma nella sentenza *CRU c. EDPS*, nella quale la Corte – pur senza discostarsi dall'orientamento precedente [268] – ha precisato che la mera esistenza di "informazioni aggiuntive" potenzialmente idonee a rendere identificabile l'interessato "non implica, di per sé, che dati

---

Applicando tale principio al caso concreto, la Corte ha ritenuto innegabile che i commenti forniti dai portatori di interesse e dai creditori costituiscano dati personali, in quanto espressione delle loro opinioni. Secondo i giudici, infatti, le opinioni personali, essendo manifestazione del pensiero di una persona, sono "necessariamente strettamente connessi" a quest'ultima (punto 58).

[266] La definizione di dati relativi alla salute contenuta all'art. 4, n. 15, GDPR (e al considerando 35) non contribuisce certamente a fare chiarezza, qualificando tali dati, *in primis*, come dati personali "attinenti" alla salute fisica o mentale. In questo modo, il legislatore sembrerebbe richiedere un collegamento diretto tra le informazioni e l'interessato. Al tempo stesso però la medesima disposizione specifica che questi dati sono tali quando "rivelano informazioni" sullo stato di salute della persona fisica, consentendo così all'interprete di ampliare le maglie del concetto in questione.

[267] Ulteriori ipotesi su come applicare il test di identificabilità sono state formulate da Dalla Corte, il quale insiste su due aspetti: i) la nozione di "mezzi che possono essere ragionevolmente utilizzati per l'identificazione" deve essere interpretata tenendo conto di fattori obiettivi (ad es. i costi e i tempi necessari per l'identificazione e la disponibilità di informazioni aggiuntive); ii) tali mezzi possono essere a disposizione non solo del titolare del trattamento, ma anche di "un terzo" (*another person*). Tuttavia, quest'ultimo non è rappresentato da qualsiasi persona, bensì solo da coloro con cui il titolare del trattamento può ragionevolmente entrare in contatto. Cfr. L. DALLA CORTE, *Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law*, in *EJLT*, 2019, vol. 10, pp. 14-16.

[268] Si veda, in particolare, la sentenza *Scania*.

pseudonimizzati debbano essere considerati, in ogni caso e per qualsiasi persona, come dati personali" [269]. Ne consegue che i dati pseudonimizzati non devono essere automaticamente qualificati come dati personali, poiché la pseudonimizzazione può, a seconda delle circostanze, "effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato in modo tale che, per esse, quest'ultimo non sia o non sia più identificabile" [270]. Rimane tuttavia fermo che chi riceve dati pseudonimizzati: i) non deve trovarsi nella condizione di poter accedere a informazioni che consentono la re-identificazione; ii) deve evitare di condividerli con soggetti che dispongono dei mezzi per re-identificare gli interessati [271].

La concezione relativa di "dato personale" ribadita dalla Corte in questa occasione ha il merito di suggerire un'interpretazione del GDPR capace di tenere insieme non solo la posizione della persona fisica, cui deve essere assicurato un elevato livello di tutela, ma anche quella dei soggetti coinvolti nel trattamento, per i quali occorre valutare in concreto le effettive possibilità di re-identificazione. Tale valutazione richiede un test di identificabilità la cui

---

[269] Sentenza *EDPS c. CRU*, punto 82. In breve, il caso riguarda la possibilità di considerare "anonimi" e, quindi, non personali, dati pseudonimizzati da colui che li trasferisce (nel caso di specie, il Consiglio di Risoluzione Unico – CRU) e non re-identificabili dal destinatario (nel caso, Deloitte). Nello specifico, secondo l'EDPS, il CRU non aveva correttamente informato azionisti e creditori, coinvolti in una procedura di indennizzo a seguito della risoluzione di un ente creditizio spagnolo, circa il trasferimento a Deloitte di alcune osservazioni raccolte nel corso della procedura. Benché tali dati fossero stati pseudonimizzati tramite l'attribuzione casuale di un codice alfanumerico e Deloitte non disponesse dei dati identificativi raccolti dal CRU in fase di iscrizione, l'EDPS riteneva che i dati in questione non fossero anonimi, ma solo pseudonimizzati. Pertanto, il trasferimento a un destinatario non indicato nell'informativa fornita agli interessati al momento della raccolta era da considerarsi illecito. Impugnata la decisione, il Tribunale (sentenza del 26 aprile 2023, causa T-557/20, *CRU c. EDPS*, ECLI: EU:T:2023:219), ha invece escluso che si trattasse di dati personali perché: i) non "concernenti" una persona specifica (punto 74); ii) Deloitte non aveva "un mezzo che poteva essere ragionevolmente attuato […] per identificare gli autori delle osservazioni" (punto 104). Investita del ricorso contro tale sentenza, la Corte ha sostanzialmente confermato l'orientamento del Tribunale, soprattutto in relazione al requisito dell'identificabilità. Occorre infine precisare che il caso concerne l'interpretazione della nozione di "dato personale" ai sensi del regolamento (UE) 2018/1725. Tuttavia, come osservato dalla stessa Corte, poiché tale nozione è definita in termini sostanzialmente identici nel GDPR, al fine di garantire un'applicazione uniforme e coerente del diritto dell'Unione, l'orientamento interpretativo vale in egual misura anche per il regolamento (UE) 2018/1725 (sentenza *EDPS c. CRU*, punto 52).

[270] *Ibid.* punto 86. Si tratta di un'affermazione che risulta in parte in contrasto con quanto sostenuto dall'EDPB nelle *Guidelines n. 01/2025 on pseudonymisation*, secondo le quali "*pseudonymised data can be considered anonymous only if the conditions for anonymity are met*" (p. 3). Non a caso, tali Linee guida sono attualmente oggetto di revisione, avviata a seguito dello *Stakeholder event on anonymisation and pseudonymisation in light of the EDPS v SRB judgment – discussion paper*.

[271] *Ibid.* punto 77.

natura – come evidenziato dai giudici del Kirchberg – deve necessariamente essere dinamica e contestuale [272]. In quest'ottica, le norme del GDPR vanno interpretate assumendo il punto di vista dei destinatari dei dati, senza presupporre che essi abbiano sempre a disposizione i mezzi per risalire all'identità dell'interessato [273].

L'adozione di un simile criterio nella definizione di "dato personale" – accolto anche nella proposta della Commissione contenuta nel *Digital Omnibus*, secondo cui un'informazione non è personale per un dato titolare quando questi non dispone di mezzi ragionevolmente utilizzabili per identificare la persona [274] – può certamente generare margini di incertezza, poiché un medesimo set di dati può risultare personale per alcuni soggetti e non personale per altri [275].

---

[272] A. PARZIALE, E. PULICE, D. MASCALZONI, *op. cit.*, 2025, p. 10.

[273] Per quanto riguarda il criterio della ragionevole probabilità di utilizzo dei mezzi per identificare una persona fisica, la Corte ha confermato l'orientamento espresso in *OC c. Commissione*, punto 52, ribadendo che "non si può ragionevolmente avvalere di un mezzo per identificare la persona interessata quando l'identificazione di tale persona è vietata dalla legge [si pensi al divieto di re-identificazione previsto dall'art. 61, par. 3, EHDS] o praticamente irrealizzabile, per esempio a causa del fatto che ciò implicherebbe un dispendio sproporzionato di tempo, costi e manodopera" (sentenza *EDPS c. CRU*, punto 82). Questa impostazione si colloca in continuità con la sentenza *IAB Europe*, nella quale i giudici hanno ritenuto sufficiente l'esistenza di un obbligo legale di comunicare le informazioni aggiuntive a terzi per soddisfare il criterio della ragionevole probabilità di utilizzo dei mezzi di identificazione. In quel caso, la Corte ha stabilito che una stringa di caratteri e lettere potesse costituire dato personale, poiché la IAB Europe disponeva dei mezzi ragionevoli per risalire all'identità dell'utente: i membri dell'associazione erano infatti tenuti, su sua richiesta, a trasmettere tutte le informazioni necessarie per procedere all'identificazione degli utenti (sentenza *IAB Europe*, punto 48. Per una ricostruzione dei fatti della causa, v. sezione 2.1). Non si fa alcun riferimento, invece, ai "fattori obiettivi" del considerando 26 GDPR, secondo i quali la valutazione sulla ragionevole probabilità di identificazione deve tenere conto di costi e tempi necessari, nonché delle tecnologie disponibili al momento del trattamento e dei successivi sviluppi tecnologici. Tali criteri, introdotti nel GDPR, su suggerimento del WP, erano stati ulteriormente integrati nel parere n. 04/2007 con altri elementi, tra cui: la finalità del trattamento; le modalità di strutturazione dello stesso; il vantaggio atteso del titolare; gli interessi dei singoli; il rischio di disfunzioni organizzative o tecniche.

[274] Art. 3, par. 1, lett. a), *Digital Omnibus*. Al riguardo, la proposta di modifica al GDPR attribuisce inoltre alla Commissione il compito di definire criteri e modalità per determinare quando i dati pseudonimizzati cessino di essere qualificati come dati personali, tenendo conto del rischio di reidentificazione e dello stato dell'arte tecnologico (art. 3, par. 10, *Digital Omnibus*). In tal modo, la Commissione verrebbe ad assumere un ruolo determinante nella delimitazione dell'ambito di applicazione sostanziale della disciplina in esame, profilo che, pur esulando dall'oggetto del presente contributo, solleva non trascurabili perplessità, segnatamente sotto il profilo della legittimità.

[275] In questo senso, cfr. A. LODIE, *Are Personal Data Always Personal? Case T-557/20 SRB v. EDPS or When the Qualification of Data Depends on Who Holds Them*, in *European Law Blog*, 2023.

Cionondimeno, tale prospettiva appare più coerente con gli obiettivi del GDPR e più aderente alle esigenze della società contemporanea, specialmente nei settori sanitario e della ricerca medico-scientifica. In questi ambiti, infatti, è frequente che i dati vengano pseudonimizzati da un soggetto (ad es. un centro di ricerca o un'azienda sanitaria) e trasmessi a un altro soggetto (ad es. una società farmaceutica o un'università) che finanzia o coordina le attività di trattamento.

Tradizionalmente, tali dati erano considerati pseudonimizzati e dunque ricompresi nell'ambito di applicazione del GDPR. La pronuncia della Corte introduce invece un approccio più pragmatico, che impone di verificare, in concreto, se il destinatario sia realmente in grado di effettuare una re-identificazione. In questo modo, viene superata l'idea secondo cui la semplice possibilità di re-identificazione comporti automaticamente la qualificazione dei dati come personali, aprendo alla possibilità di considerare anonimi dati che, in precedenza, sarebbero stati ritenuti pseudonimizzati.

Infine, i criteri interpretativi stabiliti dalla Corte contribuiscono a chiarire la distinzione tra dato anonimo e pseudonimo, fondamentale anche per la realizzazione degli obiettivi perseguiti dallo EHDS. Per l'uso secondario dei dati sanitari, infatti, il legislatore europeo incoraggia il ricorso a tecniche di anonimizzazione e pseudonimizzazione da parte degli organismi responsabili dell'accesso ai dati [276], pur avvertendo dei rischi di re-identificazione connessi all'uso di tecniche di anonimizzazione, soprattutto in relazione alle malattie rare. In questi casi, il numero esiguo di soggetti coinvolti rende difficile un'aggregazione completa dei dati, ponendo il problema di conciliare la tutela della privacy delle persone fisiche con la necessità di mantenere un livello di granularità sufficiente affinché i dati rimangano significativi [277].

3.2.2. Alcune ipotesi alternative di bilanciamento nell'interpretazione dei mezzi di conciliazione

Se da un lato l'individuazione di alternative interpretative per quanto riguarda il campo di applicazione materiale del GDPR è almeno in parte ostacolata dall'uso di termini generici nella definizione di concetti chiave della disciplina [278], dall'altro potrebbero esserci maggiori margini di manovra con

[276] Art. 66, parr. 2-3, EHDS.

[277] Considerando 92 EHDS.

[278] A tale proposito, anziché per via interpretativa, i limiti evidenziati nella sezione precedente potrebbero essere superati più efficacemente tramite una revisione del GDPR. Questo tema, anche se limitatamente alle disposizioni del GDPR sui trattamenti di dati personali ai fini di ricerca scientifica, verrà esaminato in modo più approfondito all'interno della sezione 3.1 del capitolo 4. Fin d'ora, tuttavia, va riconosciuto che, nel quadro del *Digital Omnibus*, risulta

riferimento alle disposizioni che sono state volutamente inserite per conciliare il diritto individuale alla protezione dei dati personali con altri diritti e interessi tutelati dal GDPR. In questi casi, è fondamentale evitare automatismi nelle operazioni di bilanciamento che implicano il prevalere del diritto individuale alla protezione dei dati personali per regola, sulla base di obiettivi del GDPR che sembrano essere stati fraintesi. Piuttosto, il bilanciamento dovrebbe essere condotto attraverso una valutazione in concreto dei diritti e degli interessi in gioco, applicando sistematicamente il principio di proporzionalità.

Come osservato in precedenza, tra le disposizioni che possono essere considerate mezzi di conciliazione, vi sono quelle relative al diritto di accesso ai dati. Sebbene la Corte abbia offerto un'interpretazione ampia della portata di questo diritto, in virtù del legame con il principio di trasparenza [279] e alla luce degli obiettivi del GDPR [280], i giudici hanno anche riconosciuto la possibilità che il diritto di accesso ai dati subisse limitazioni. Ciò avviene, ad esempio, quando è "impossibile comunicare l'identità dei destinatari concreti, in particolare qualora questi ultimi non siano ancora noti", e quando il titolare dimostra, conformemente al principio di responsabilità, che la richiesta di accesso ai dati è "manifestamente infondata o eccessiva" [281]. Così facendo, si

---

apprezzabile lo sforzo della Commissione di proporre una definizione di "dato personale" che valorizzi un criterio soggettivo e non assoluto, nel tentativo di contenere la progressiva espansione di tale nozione e, di conseguenza, dell'ambito di applicazione del GDPR (art. 3, par. 1, lett. a), *Digital Omnibus*). Ciononostante, una simile restrizione, potendo – come evidenziato nel parere congiunto dell'EDPB e dell'EDPS 2/2026 – incidere sul diritto fondamentale alla protezione dei dati personali, avrebbe forse meritato una collocazione diversa, non essendo pienamente coerente con la natura di un pacchetto normativo che dovrebbe limitarsi a introdurre modifiche puntuali e di carattere meramente tecnico.

[279] Sentenze *FT (Copie di cartelle cliniche)*, punto 43; *Pankki S*, punto 52; *Osterreichische Datenschutzbehörde e CRIF*, punti 36-38; *RW c. Österreichische Post AG*, punto 35.

[280] Cfr. sentenza *Pankki S*, dove la Corte ha affermato che il diritto di accesso include anche le informazioni relative alle persone che effettuano operazioni di trattamento, al fine di "assicurare un livello coerente ed elevato di protezione delle persone fisiche all'interno dell'Unione nonché di rafforzare e di disciplinare in modo dettagliato i diritti degli interessati" (punto 55); sentenza *RW c. Österreichische Post AG*, in cui si stabilisce che consentire all'interessato di accedere alle informazioni relative ai destinatari delle comunicazioni contenenti dati personali (e non solo alle categorie di destinatari) contribuisce al raggiungimento dell'obiettivo del GDPR di "garantire un elevato livello di protezione delle persone fisiche all'interno dell'Unione", dando attuazione "alle prescrizioni scaturenti dal diritto fondamentale alla protezione dei dati personali tutelato dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, in particolare alle prescrizioni espressamente previste al paragrafo 2 di tale articolo" (punto 44).

[281] Sentenza *RW c. Österreichische Post AG*, punti 48-49. Similmente, nella successiva sentenza *Pankki S*, la Corte sottolinea che riconoscere un'ampia portata al diritto di accesso non implica necessariamente l'accesso "alle informazioni relative all'identità dei dipendenti di detto titolare che hanno svolto tali operazioni sotto la sua autorità e conformemente alle sue istruzioni, a meno che tali informazioni siano indispensabili per consentire all'interessato di

dovrebbe assicurare un equilibrio tra il diritto di accesso dell'interessato e gli oneri imposti al titolare del trattamento.

Tuttavia, nella giurisprudenza della Corte, tale equilibrio è stato proiettato a favore di una maggiore attenzione verso la tutela della protezione dei dati e della vita privata dell'interessato, a discapito della posizione giuridica dei titolari del trattamento, i quali sono portatori di propri interessi economici, ma anche talvolta degli interessi della collettività. In ragione della rilevanza economica e sociale delle attività di trattamento di dati personali, ogni operazione di bilanciamento dovrebbe richiedere un'accurata analisi e ponderazione dei diritti e degli interessi in gioco, tenendo conto anche dell'impatto che la protezione delle prerogative degli interessati può avere sulla società nel suo complesso.

In questo senso, è apprezzabile lo sforzo compiuto dai giudici di Lussemburgo in *Rijkeboer*, nel cercare di offrire un'interpretazione che non penalizzasse eccessivamente il titolare del trattamento. In quell'occasione, la Corte ha ammesso che la limitazione prevista dalla legge olandese al diritto di accesso ai dati avrebbe potuto considerarsi legittima qualora si fosse dimostrato che un periodo di conservazione più lungo dei dati avrebbe posto un onere sproporzionato sul titolare del trattamento [282]. In tal caso, la Corte avrebbe potuto ritenere che l'obbligo di conservazione dei dati imposto dal diritto nazionale al titolare fosse effettivamente adeguato a garantire un giusto equilibrio tra la tutela dell'interessato e quella del titolare.

Cionondimeno, come già evidenziato, la giurisprudenza successiva non ha seguito questa linea [283]. In *FT*, ad esempio, i giudici non hanno spiegato perché gli interessi economici del titolare non dovrebbero rientrare tra i diritti e le libertà che consentono di ammettere limitazioni al diritto di accesso ai sensi degli artt. 15, par. 4, GDPR o 23, par. 1, lett. i), GDPR (nel caso di specie, la facoltà di porre a carico del paziente le spese sostenute per soddisfare le richieste di copie). Non viene nemmeno chiarito come gli interessi economici del titolare possono ledere l'essenza dei diritti fondamentali dell'interessato, né i criteri per valutare se una misura è necessaria e proporzionata in una società democratica, come previsto dall'art. 23 GDPR.

Al contrario, nella stessa causa, l'Avvocato generale Emiliou ha esaminato attentamente le condizioni stabilite dall'art. 23, par. 1, GDPR (e dall'art. 52 della Carta) per valutare l'ammissibilità della normativa nazionale. Per i fini che qui interessano, riteniamo opportuno ripercorrere la sua argomentazione

---

esercitare effettivamente i diritti che gli sono conferiti da tale regolamento e a condizione che si tenga conto dei diritti e delle libertà di tali dipendenti" (punto 83). Cfr. anche la sentenza della Corte del 19 marzo 2026, causa C-526/24, *Brillen Rottler*, ECLI:EU:C:2026:216, punto 30.

[282] Sentenza *Rijkeboer* punto 66.

[283] Cfr. sezione 2.2.

poiché propone un'interpretazione delle norme del GDPR che tiene maggiormente conto dei diritti e degli interessi diversi da quelli dell'interessato.

Per prima cosa, l'Avvocato generale ha affermato che la restrizione al diritto di accesso ai dati è disciplinata "in una misura legislativa" [284] e la sua "natura relativamente innocua" non compromette l'"essenza" di tale diritto, perché "non priva gli individui del *nucleus durus* del loro diritto alla protezione dei dati" [285]. Tale normativa persegue altresì obiettivi contemplati dall'art. 23, par. 1, lett. e) e i), GDPR e, più in generale, dal diritto dell'Unione. Da un lato, infatti, il limite posto dalla normativa nazionale mira a preservare la sanità pubblica, in linea con l'art. 35 della Carta e l'art. 8, par. 2, CEDU [286]. Dall'altro, tale limite si propone di proteggere alcuni diritti economici fondamentali dei titolari, come la libertà professionale e il diritto di lavorare, la libertà di impresa e il diritto di proprietà [287]. Scoraggiando le richieste superflue o futili di copie, la misura nazionale consente di tutelare gli interessi economici dei medici e, così, garantire che essi dedichino la maggior parte del proprio tempo alle mansioni fondamentali di carattere sanitario, anziché occuparsi di compiti amministrativi evitabili [288].

Da ultimo, è stato osservato che l'obbligo per gli interessati di sostenere i costi amministrativi connessi alla produzione delle copie richieste è idoneo a dissuaderli dall'avanzare richieste di accesso superflue o futili [289], senza eccedere quanto necessario per tutelare gli interessi economici dei medici [290]. È

---

[284] Conclusioni dell'Avvocato generale Emiliou del 20 aprile 2023, causa C-307/22, *FT (Copie di cartelle cliniche)*, ECLI:EU:C:2023:315, punto 38.

[285] *Ibid.* punto 40.

[286] *Ibid.* punto 43.

[287] Artt. 15-17 della Carta. Con riferimento a questi diritti, l'Avvocato generale sottolinea come il GDPR tuteli tutti i diritti fondamentali, compresi i diritti di natura economica che, quindi, non possono essere considerati "figli di un dio minore" rispetto ai diritti civili, sociali o politici (punto 48).

[288] Conclusioni dell'Avvocato generale Emiliou in *FT (Copie di cartelle cliniche)*, punto 48.

[289] *Ibid.* punto 54.

[290] *Ibid.* punto 65. A questo proposito, l'Avvocato generale ha giudicato irragionevole la proposta avanzata dalla Commissione sulla possibilità di introdurre, come misura alternativa meno restrittiva della tutela nei confronti del diritto alla protezione dei dati degli individui, un regime differenziato a seconda della dimensione del titolare del trattamento. Per la Commissione, infatti, l'approccio unico adottato dal legislatore tedesco potrebbe non essere necessario a tutelare gli interessi economici dei medici, qualora questi ultimi operino all'interno di grandi studi medici, di ospedali e di cliniche private che, solitamente, dispongono di personale e attrezzature dedicate a svolgere tutte le mansioni di carattere amministrativo connesse all'erogazione di prestazioni sanitarie. Lo stesso vale per quei medici che possono recuperare i costi aggiuntivi sostenuti per gestire le richieste di accesso ai dati aumentando le tariffe. Queste considerazioni dovrebbero portare all'elaborazione di una disciplina differenziata che, tuttavia, secondo l'Avvocato generale introdurrebbe una complessità eccessiva, specialmente se si

stato anche evidenziato che la decisione di addebitare al paziente le spese sostenute per soddisfare le richieste di copie costituisce una decisione di natura politica, che spetta al legislatore nazionale, specialmente in un settore come quello sanitario [291]. Pertanto, la valutazione della proporzionalità di tale misura nazionale non dovrebbe rientrare tra le competenze della Corte, ma del giudice del rinvio, il quale dovrà verificare che le spese rimborsabili ai medici siano strettamente limitate a quelle effettivamente sostenute per produrre e mettere a disposizione le copie richieste (ad es. la carta, la cartuccia delle stampanti o delle fotocopiatrici e/o le chiavette USB) [292].

In definitiva, l'Avvocato generale Emiliou ha riconosciuto che l'art. 23, par. 1, GDPR permette al diritto nazionale di imporre ai pazienti che richiedono copie dei loro dati personali contenuti nelle cartelle cliniche di rimborsare ai medici i costi sostenuti, purché il giudice del rinvio accerti che la restrizione al diritto di accesso sia necessaria e proporzionata agli obiettivi di tutela della sanità pubblica e della libertà di impresa dei medici. All'opposto, la decisione della Corte ha escluso a priori questa possibilità [293], con potenziali conseguenze negative su alcune norme nazionali esistenti che consentono di subordinare l'esercizio del diritto di accesso al pagamento di una somma di denaro al fine di tutelare altri interessi in gioco [294].

Alla luce di tali considerazioni, dunque, un'interpretazione del diritto di accesso ai dati e, più in generale, dei diritti dell'interessato più rispettosa degli obiettivi del GDPR dovrebbe consentire limitazioni ogni qualvolta si accerti, tramite una valutazione in concreto basata sul principio di proporzionalità,

---

considera l'esiguo importo che viene solitamente richiesto ai pazienti. Inoltre, gli Stati membri non possono essere obbligati a prevedere, ai fini della proporzionalità, misure alternative che potrebbero rappresentare un onere eccessivo per gli stessi e potrebbero altresì avere l'effetto di incoraggiare i pazienti a rivolgersi a cliniche più grandi che forniscono gratuitamente copie delle cartelle cliniche piuttosto che a studi più piccoli che chiedono il pagamento di un importo supplementare per tali copie (punti 61-63).

[291] *Ibid.* punto 68.

[292] *Ibid.* punti 69-70.

[293] A questo proposito, sarebbe stato opportuno che la Corte motivasse perché la libertà d'impresa non può considerarsi rilevante nell'interpretazione dell'art. 23, par. 1, lett. i), GDPR, dal momento che il GDPR non specifica in modo esplicito cosa debba rientrare tra "i diritti e gli interessi altrui" che possono limitare l'esercizio del diritto all'accesso ai dati personali. L'unica indicazione è fornita dal considerando 63 GDPR, che riconduce nell'ambito di applicazione di tale disposizione il segreto industriale e la proprietà intellettuale. A questo proposito, nemmeno le linee guida dell'EDPB contribuiscono a fare chiarezza (linee guida n. 10/2020 sulle limitazioni a norma dell'art. 23, regolamento (UE) 2016/679, punti 33-34).

[294] In Italia, ad esempio, l'art. 25, par. 1, legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e diritto di accesso ai documenti amministrativi, prevede che "[i]l rilascio di copia è subordinato soltanto al rimborso del costo di riproduzione, salve le disposizioni vigenti in materia di bollo, nonché i diritti di ricerca e di visura".

che: i) il titolare abbia fornito opportune garanzie agli interessati (*in primis*, l'uso di mezzi che consentano loro di essere informati rispetto alle operazioni di trattamento) [295]; ii) senza queste restrizioni, il titolare, in quanto portatore di interessi individuali o collettivi, subirebbe un sacrificio eccessivo delle proprie prerogative.

Oltre al diritto di accesso ai dati, nella sezione 2.2, abbiamo preso in considerazione anche l'art. 9 GDPR come mezzo di conciliazione, poiché contiene, al secondo paragrafo, una serie di ipotesi derogatorie al divieto generale di trattamento dei dati sensibili che dovrebbero permettere di contemperare il diritto individuale alla protezione dei dati personali con altri diritti e interessi in gioco. Tuttavia, l'orientamento giurisprudenziale consolidato su questa disposizione rischia di limitare le possibilità che la stessa normativa riconosce ai titolari del trattamento di svolgere le proprie attività, a discapito non solo dei loro interessi, ma anche potenzialmente di quelli della collettività. Alla luce di una rilettura degli obiettivi del GDPR e degli sviluppi normativi interventi dalla sua adozione, riteniamo che siano possibili alternative interpretative.

In primo luogo, pur senza negare che le eccezioni di cui all'art. 9, par. 2, GDPR debbano essere interpretate restrittivamente, il divieto generale stabilito al primo paragrafo dell'art. 9 GDPR non dovrebbe "determinare una riduzione dell'ambito di applicazione di un'altra disposizione di tale regolamento in modo contrario al chiaro tenore letterale di quest'ultima" [296]. In altre parole, una lettura restrittiva delle ipotesi derogatorie previste all'art. 9, par. 2, GDPR, giustificata dalla presenza di un divieto generale di trattamento dei dati sensibili, non può pregiudicare l'effetto utile delle autorizzazioni al trattamento contenute in questa norma. In particolare, le giustificazioni di cui all'art. 9, par. 2, GDPR non dovrebbero essere interpretate in modo da introdurre requisiti aggiuntivi a tutela delle ragioni dell'interessato che non emergono chiaramente dall'analisi testuale della disposizione in oggetto [297].

---

[295] Ulteriori misure di garanzia possono essere: i) concedere all'interessato la possibilità di revocare il proprio consenso, ii) limitare la quantità di dati raccolti, iii) cancellare immediatamente i dati dopo il loro utilizzo, iv) utilizzare tecniche di anonimizzazione.

[296] Così si è espressa la Corte stessa in una causa dove si è pronunciata, tra le altre cose, sulla portata dell'art. 9, par. 2, lett. h), GDPR. Cfr. sentenza *Krankenversicherung Nordrhein*, punto 51.

[297] Nel caso di specie, la Corte ha sottolineato che restringere l'ambito di applicazione dell'art. 9, par. 2, lett. h), GDPR solo ai casi in cui un terzo neutrale tratta i dati per valutare la capacità lavorativa di un lavoratore introdurrebbe un requisito che non si deduce dal tenore letterale di questa norma. Un'interpretazione diversa sarebbe contraria agli obiettivi dell'art. 9 e, più in generale, del GDPR. Richiamando il considerando 4 GDPR, si sottolinea che il diritto alla protezione dei dati personali non è una prerogativa assoluta e deve essere contemperato con altri diritti fondamentali in conformità con il principio di proporzionalità, anche

In secondo luogo, sarebbe opportuno riconsiderare la soluzione cumulativa proposta dal WP, secondo cui, in caso di trattamento di dati sensibili, il titolare deve dimostrare la presenza di una base giuridica non solo tra quelle dell'art. 9, par. 2, GDPR, ma anche tra quelle dell'art. 6, par. 1, GDPR [298]. Sebbene anche la Corte abbia riconosciuto che l'art. 6, par. 1, GDPR debba essere rispettato in tutti i trattamenti, anche quelli relativi ai dati sensibili [299], e così anche la dottrina maggioritaria [300], come osservato dall'Avvocato generale Campos Sánchez Bordona in *Krankenversicherung Nordrhein*, guardando alla genesi dell'art. 9 GDPR, il rapporto tra le due norme è tutt'altro che pacifico [301].

Il testo del GDPR potrebbe essere interpretato in modo che l'art. 9, par. 2, GDPR costituisca una *lex specialis* della regola generale fissata dall'art. 6, par. 1, GDPR per i trattamenti di dati comuni [302]. Quest'ultima, infatti, non viene richiamata esplicitamente dall'art. 9, par. 2, GDPR e il fatto che il trattamento di categorie particolari di dati debba essere rispettoso dei principi di cui all'art. 5 GDPR, tra cui il principio di liceità [303], non implica automaticamente la necessità di cumulare le condizioni presenti negli artt. 6, par. 1, e 9, par. 2, GDPR. Piuttosto, vista la peculiarità dei dati in questione, dovrebbe essere sufficiente basare il trattamento su una delle condizioni di cui all'art. 9, par. 2, GDPR, le quali sono state introdotte proprio per costituire il fondamento normativo di specifiche attività di trattamento e sono pensate come eccezioni al divieto generale posto dal primo paragrafo dell'art. 9 GDPR.

Una possibile obiezione alla tesi della non cumulabilità tra gli artt. 6 e 9 GDPR è che essa produrrebbe un paradosso in quelle ipotesi in cui l'art. 9

---

qualora vengano utilizzate categorie particolari di dati (sentenza *Krankenversicherung Nordrhein*, punti 51 e 54-57).

[298] Parere del WP n. 06/2014, e così anche le linee guida dell'EDPB n. 03/2020, p. 23.

[299] Cfr. *inter alia*, sentenza *Krankenversicherung Nordrhein*, punti 78-79.

[300] Tra coloro che ritengono che le basi giuridiche di cui all'art. 6, par. 1, GDPR e all'art. 9, par. 2, GDPR devono essere fornite entrambe qualora i dati sanitari vengano trattati, cfr. J.C. CHEN, E.S. DOVE, H. BHAKUNI, *Explicit Consent and Alternative Data Protection Processing Grounds for Health Research*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022, p. 483, e G. COMANDÉ, G. SCHNEIDER, *Differential Data Protection Regimes in Data-driven Research: Why the GDPR is More Research-friendly Than You Think*, in *Ger. Law J.*, 2022(a), vol. 23, n. 4, p. 570.

[301] Conclusioni dell'Avvocato generale Campos Sánchez Bordona in *Krankenversicherung Nordrhein*, punti 58-59.

[302] Ipotesi interpretativa che è stata riconosciuta, ad esempio, da B. BELORTAJA, *Less is More: The Redundant Application of Articles 6(1) and 9(1)(2) GDPR in* Krankenversicherung Nordrhein *(C-667/21)*, in *EU Law Live*, 2024; G. FRANCO, F. SARTORE, *Art. 9*, in L. BOLOGNINI, E. PELINO, *Codice della disciplina privacy*, Giuffrè, Milano, 2024, p. 110.

[303] Art. 5, par. 1, lett. a), GDPR.

GDPR sembrerebbe offrire una tutela meno garantista rispetto all'art. 6 GDPR. Si pensi, in particolare, al caso del trattamento dei dati sensibili "resi manifestamente pubblici" dall'interessato, che consente di derogare al divieto generale di cui all'art. 9, par. 1, GDPR [304], senza che esista una corrispondente base giuridica per i dati comuni nell'art. 6, par. 1, GDPR. Tuttavia, questa obiezione non risulta convincente. Il fatto che la pubblicazione volontaria di dati sensibili possa legittimare il trattamento ai sensi dell'art. 9, par. 2, lett. e), GDPR non implica un abbassamento del livello di protezione tale da richiedere l'ulteriore ricorso alle basi giuridiche dell'art. 6, par. 1, GDPR. Al contrario, si tratta di una modulazione della tutela fondata sul principio di autodeterminazione informativa, secondo cui l'interessato può consapevolmente rinunciare, in casi eccezionali, alla protezione rafforzata normalmente prevista per i dati appartenenti alle categorie particolari.

Questa rinuncia, tuttavia, non è presunta né automatica. La Corte ha infatti chiarito che l'eccezione dell'art. 9, par. 2, lett. e), GDPR, può essere invocata solo qualora "l'interessato abbia inteso, in modo esplicito e con un atto positivo chiaro, rendere accessibili al pubblico i dati" in questione [305]. Non è sufficiente la semplice interazione con un sito o un'applicazione, né l'inserimento passivo di informazioni online: è necessario che l'utente abbia potuto effettuare una scelta informata sull'accessibilità dei propri dati, attraverso un'impostazione individuale dei parametri di visibilità, oppure che abbia espresso un consenso esplicito alla pubblicazione in un contesto chiaramente informato [306].

Alla luce di questa interpretazione, è evidente che l'art. 9, par. 2, lett. e), GDPR non apre a una generalizzata liberalizzazione del trattamento dei dati sensibili, ma prevede una deroga attentamente circoscritta, che continua a essere soggetta ai principi fondamentali di cui all'art. 5 GDPR. L'apparente asimmetria rispetto ai dati comuni, dunque, non giustifica la necessità di cumulare anche una base giuridica *ex* art. 6, par. 1, GDPR. Si tratta piuttosto del riflesso di una diversa impostazione normativa, in cui le condizioni dell'art. 9, par. 2, GDPR fungono da basi giuridiche autonome per il trattamento dei dati sensibili in contesti eccezionali e chiaramente delimitati.

Cionondimeno, qualora la tesi della non cumulabilità dovesse rimanere minoritaria [307], si dovrebbe almeno tentare di superare l'idea che il consenso

---

[304] Art. 9, par. 2, lett. e), GDPR.

[305] Sentenza *Meta Platforms e a.*, punto 77.

[306] *Ibid.* punti 81-83.

[307] Similmente, anche il legislatore europeo, con lo EHDS, ha confermato l'opzione cumulativa, specificando che la base giuridica dei trattamenti di dati sanitari elettronici effettuati nell'ambito dello EHDS è rappresentata dagli artt. 6, par. 1, a), c), e) o f) e 9, par. 2, g)-j). Cfr. capitolo 4, sezione 3.

rappresenta la base giuridica per eccellenza. Tale interpretazione non trova riscontro né nel GDPR, dove l'art. 6, par. 1, stabilisce che "il trattamento è lecito solo se e nella misura in cui ricorre *almeno una delle* seguenti condizioni", né nella Carta, il cui art. 8, par. 2, precisa che i dati personali devono essere trattati "in base al consenso della persona interessata *o a un altro* fondamento legittimo previsto dalla legge" [308]. Benché, dunque, a livello normativo, non esista una gerarchia tra le basi giuridiche di cui all'art. 6 GDPR [309], nella pratica, il ricorso al consenso viene spesso privilegiato, in quanto considerato il "*best way for individuals to control data processing activities*" [310].

In realtà, questo controllo è spesso illusorio [311]. Basti pensare, ad esempio,

---

[308] Corsivo aggiunto.

[309] Nel parere del WP n. 06/2014, il WP afferma che "il testo della direttiva non opera una distinzione giuridica tra i sei criteri di liceità del trattamento né suggerisce l'esistenza di una gerarchia fra loro. Non esistono indicazioni secondo cui l'articolo 7, lettera f), deve essere applicato solo in casi eccezionali né dal testo si evince altrimenti che l'ordine specifico dei sei fondamenti giuridici avrà effetti giuridicamente vincolanti" (p. 12). In questo senso, v. anche il parere del WP n. 15/2011 sulla definizione di consenso, WP 187; le linee guida dell'EDPB n. 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19, 2020, p. 6; le linee guida dell'EDPB n. 05/2020; la decisione vincolante dell'EDPB n. 05/2022 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Meta Platforms Ireland Limited (Instagram) ai sensi dell'art. 65, par. 1, lett. a), regolamento (UE) 2016/679, punto 100; il parere dell'EDPB n. 28/2024 su alcuni aspetti della protezione dei dati relativi al trattamento dei dati personali nel contesto dei modelli di IA, punto 60. In senso analogo, gran parte della dottrina ha evidenziato che né la DPD né il GDPR individuano il consenso come base giuridica prioritaria, e che il GDPR, oltre a porre una serie di condizioni affinché il consenso possa essere considerato una base giuridica valida, facilita il ricorso a condizioni di liceità alternative. Cfr., *inter alia*, L.A. BYGRAVE, D. WIESE SCHARTUM, *Consent, Proportionality and Collective Power*, in S. GUTWIRTH et al. (eds.), *op. cit*., 2009, pp. 157-174 e N. PURTOVA, *op. cit*., 2014(a), p. 14.

[310] Cfr. la relazione della commissione LIBE sul regolamento generale sulla protezione dei dati, 2013, p. 200. Inoltre, il WP, nel parere n. 03/2013, sottolinea che, oltre al consenso, anche il principio di limitazione delle finalità rappresenta "*an unavoidable prerequisite of individual control, as the latter can be meaningfully exercised through consent or the right to object only if the data subject 'fully understands the purposes of processing*" (parere n. 03/2013 sulla limitazione delle finalità, WP 203, pp. 14-15). Sul significato del principio di limitazione delle finalità, v. H.B. BENTZEN, *Context as Key: The Protection of Personal Integrity by Means of the Purpose Limitation Principle*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022, p. 381 ss.; T.H.A. WISMAN, R.J.L.TIJM, *The Radical Reframing of the Purpose Limitation Principle – Why the Dutch Delegation Uprooted Data Protection*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022, p. 354 ss.; N. FORGÓ, S. HÄNOLD, B. SCHÜTZE, *The Principle of Purpose Limitation and Big Data*, in M. CORRALS, M. FENWICK, N. FORGÓ, *New Technology, Big Data and the Law*, Springer, Singapore, 2017, p. 26.

[311] A. MANTELERO, *The Future of Consumer Data Protection in the EU Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, in *Comput. Law Secur. Rev.*, 2014, n. 6, p. 643.

alle situazioni caratterizzate da una marcata asimmetria tra le parti [312], come quelle in cui il consenso è prestato a un operatore di *social network* che occupa una posizione dominante sul mercato rilevante. In questi casi, sebbene tale posizione non escluda a priori il ricorso al consenso [313], è necessario verificare che la posizione dominante dell'operatore del *social network* non comprometta il soddisfacimento delle condizioni di cui all'art. 7 GDPR [314] e che i diritti degli utenti (ad es. il diritto di rifiutare il consenso a operazioni di trattamento non necessarie per l'esecuzione del contratto) siano rispettati [315].

Di illusorietà del consenso si parla anche in riferimento ai trattamenti di dati personali per finalità di ricerca scientifica [316]. Poiché non è possibile definire con precisione come e per quali finalità specifiche verranno utilizzati i dati, è difficile per i titolari del trattamento dimostrare che il consenso ottenuto soddisfi le

---

[312] Cfr. art. 7 e considerando 43 GDPR, nonché le linee guida dell'EDPB n. 05/2020, p. 17; il parere del WP n. 15/2011, p. 6-8; il parere del WP n. 06/2014, pp. 9, 10, 13 e 14. Inoltre, vale la pena ricordare che la proposta originaria del GDPR (art. 7, par. 4) non permetteva di utilizzare il consenso nel caso in cui vi fosse "un notevole squilibrio tra la posizione dell'interessato e del responsabile del trattamento". Per un approfondimento sull'uso del consenso come base giuridica dei trattamenti online, cfr. B-J. KOOPS, *op. cit*., 2014, pp. 3-4; D.J. SOLOVE, *Privacy Self-Management and the Consent Paradox*, in *Harv. Law Rev.*, 2013, vol. 126, p. 1880. Inoltre, un vasto filone dottrinale ha sottolineato che non solo le asimmetrie informative, ma anche l'assenza di informazioni, rendono il controllo sui dati, anche tramite il consenso, fittizio. Cfr. A. ACQUISTI, J. GROSSKLAGS, *What Can Behavioral Economics Teach Us About Privacy*, in A. ACQUISTI et al. (eds.), *Digital Privacy. Theory, Technologies, and Practices*, New York, Auerbach Publications, 2008, pp. 363-377; S. TREPTE et al., *Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)*, in S. GUTWIRTH, R. LEENES, P. DE HERT (eds.), *op. cit*., 2014, pp. 333-365.

[313] Sentenza *Meta Platforms e a*., punto 147.

[314] *Ibid.* punto 148.

[315] In particolare, la Corte ha sottolineato che l'esercizio di tali diritti non deve pregiudicare la possibilità per gli utenti di fruire del servizio offerto dall'operatore del *social network* online. Se ciò non fosse possibile, agli utenti spetterebbe in ogni caso l'offerta, "se del caso a fronte di un adeguato corrispettivo, [di] un'alternativa equivalente non accompagnata da simili operazioni di trattamento di dati" (sentenza *Meta Platforms e a*., punto 150).

[316] Tra gli altri, v. Centro di Coordinamento Nazionale dei Comitati Etici (CCNCE), Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale, 2023, pp. 18-20; E. VAYENA, A. BLASIMME, *Biomedical Big Data: New Models of Control Over Access, Use and Governance*, in *Bioethical Inquiry*, 2017, vol. 14, p. 504; M. MOSTERT et al., *Big Data in Medical Research and EU Data Protection Law: Challenges to the Consent or Anonymise Approach*, in *Eur. J. Hum. Genet.*, 2016, vol. 24, pp. 956-960; L. AUSTIN, *Enough About Me: Why Privacy is About Power, Not Consent (or Harm)*, in A. SARAT (ed.), *A World Without Privacy: What Law Can and Should Do?*, CUP, Cambridge, 2014, pp. 131-189; B-J. KOOPS, *op. cit.*, 2014, p. 250; G. ZANFIR-FORTUNA, *op. cit*., 2014. Di opinione opposta sono, invece, J.C. CHEN, E.S. DOVE, H. BHAKUNI, *op. cit*., 2022, p. 481 ss.; E.S. DOVE, J.C. CHEN, *Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis*, in *Int. Data Priv. Law*, 2020, vol. 10, n. 1, p. 117.

condizioni stabilite *ex lege* (ad es. l'essere esplicito, specifico e informato) [317], specialmente alla luce dell'interpretazione restrittiva data al considerando 33 GDPR [318], che non permette al titolare "*to navigate around the key principle of specifying purposes for which consent of the data subject is asked*" [319]. In tutte queste situazioni, sarebbe preferibile utilizzare altre basi giuridiche [320], come

[317] Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche, 2007, WP 131, p. 9. Cfr. E.S. DOVE, *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in *J. Law Med. Ethics*, 2018, vol. 46, p. 1013 e M.J. TAYLOR, T. WHITTON, *Public Interest, Health research and Data Protection Law: Establishing a Legitimate Trade-Off Between Individual Control and Research Access to Health Data*, in *Laws*, 2020, vol. 9, n. 1, p. 8.

[318] Un'interpretazione diversa di questo considerando permetterebbe di ammettere forme di consenso ampio e modulare (per determinati settori di ricerca o parti di progetti di ricerca) nel rispetto delle norme deontologiche rilevanti. Cfr. G. COMANDÉ, *op. cit*., 2019(b), pp. 193-195.

[319] Documento dell'EDPB sulla risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario, 2021, p. 8. Secondo l'EDPB, nel caso in cui non sia possibile definire anticipatamente le finalità specifiche del trattamento, il considerando 33 deve essere interpretato nel senso che il titolare deve comunque assicurarsi che "*the essence of data subject's rights*" sia rispettata tramite, ad esempio, la presenza di garanzie di trasparenza o altre misure di garanzia *ex* art. 89, par. 1, GDPR, come il rispetto dei principi di minimizzazione, di integrità e riservatezza e della protezione *by design* e *by default*. Tuttavia, l'EDPB stesso riconosce che non è chiaro quali siano esattamente le ulteriori garanzie richieste dal GDPR (p. 12 e le linee guida del WP sulla trasparenza, 2017, WP 260 rev. 01, 2018, p. 31). Quale indicazione in più è stata fornita dall'EDPS in *A Preliminary Opinion on Data Protection and Scientific Research*, 2020, pp. 24 e 26, dove vengono considerate garanzie adeguate: il rispetto degli standard etici professionali; la valutazione d'impatto; la designazione di un responsabile della protezione dei dati personali; la notifica di una violazione dei dati; la sicurezza dei dati; la minimizzazione degli stessi tramite la pseudonimizzazione o, se non compromette la ricerca, l'anonimizzazione. Inoltre, viene posta particolare enfasi sul ruolo dei comitati etici "*in ensuring that the respect of human rights, including right to data protection, is embedded in the research project from the early planning stage*".

[320] Nel documento sulla risposta alla domanda di chiarimenti della Commissione europea, *op. cit.*, 2021, p. 3 ss., l'EDPB chiarisce che non utilizzare il consenso come base giuridica del trattamento dei dati sanitari per finalità di ricerca scientifica non è incompatibile con i requisiti etici fondamentali previsti dalla Convenzione di Oviedo e dalla Dichiarazione di Helsinki. Il consenso richiesto dal GDPR, infatti, si distingue dal consenso informato *ex* art. 28, par. 2, regolamento (UE) n. 536/2014 sulla sperimentazione clinica di medicinali per uso umano, che è concepito come misura per garantire la protezione del diritto alla dignità umana e all'integrità della persona (artt. 1 e 3 della Carta). Similmente, si veda anche il parere preliminare dell'EDPS, in cui si afferma che il consenso diviene "*less appropriate in the case of collected and inferred data and especially in the case of special categories of data on which much scientific research relies*" (parere preliminare dell'EDPS sulla ricerca scientifica, p. 20). A favore dell'utilizzo di basi giuridiche diverse dal consenso, si sono espressi, *inter alia*, E. DOVE, *op. cit.*, 2018, pp. 1013-1030; G. VERHENNEMAN et al., *How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research*, in *EJHL*, 2019, vol. 27, n. 1, p. 40; P. QUINN, *The Anonymisation of Research Data – A Pyric Victory for Privacy*

l'esistenza di un obbligo legale [321], l'esecuzione di un compito di interesse pubblico [322] o la presenza di un interesse legittimo [323].

Lo stesso dovrebbe avvenire anche nei casi di trattamento per finalità di ricerca in cui esiste un evidente squilibrio tra l'interessato e il titolare del trattamento [324], rendendo quindi il consenso non liberamente prestato [325]. Questa situazione potrebbe verificarsi, ad esempio, quando l'interessato appartiene a un gruppo economicamente o socialmente svantaggiato o si trova in una situazione di dipendenza istituzionale o gerarchica e la patologia di cui soffre può essere curata solamente in caso di partecipazione ad una sperimentazione clinica [326]. Non si verifica, invece, nei casi di trattamenti condotti nell'ambito di uno studio osservazionale su una determinata popolazione, relativamente alla sintomatologia e all'evoluzione di una patologia [327].

Oltre alla mancanza di garanzie sul controllo dei propri dati per l'interessato, la decisione di fondare un trattamento per fini di ricerca scientifica sul consenso pone un problema non irrilevante anche per il titolare del trattamento. Vi è infatti il rischio che, una volta ottenuto il consenso e utilizzati i dati, l'interessato decida di revocarlo *ex* art. 7, par. 3, GDPR e, eventualmente, di esercitare il proprio diritto di cancellazione *ex* art. 17, par. 1, lett. b), GDPR [328].

---

that Should Not Be Pushed Too Hard by the EU Data Protection Framework?, in *EJHL*, 2017, vol. 24, n. 4, pp. 347-367; E.B. VAN VEEN, *Observational Health Research in Europe: Understanding the General Data Protection Regulation and Underlying Debate*, in *Eur. J. Cancer*, 2018, vol. 104, pp. 70-80; P. QUINN, L. QUINN, *Big Genetic Data and its Big Data Protection Challenges*, in *Comput. Law Secur. Rev.*, 2018, vol. 34, n. 5, p. 1013.

[321] Art. 6, par. 1, lett. c), GDPR.

[322] Art. 6, par. 1, lett. e), GDPR.

[323] Art. 6, par. 1, lett. f), GDPR.

[324] Considerando 43 GDPR.

[325] Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche, 2007, p. 8 chiarisce che la persona deve essere "veramente libera di scegliere" e deve potere ritirare in un secondo momento il consenso "senza venire danneggiata".

[326] Parere dell'EDPB n. 03/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati, che rinvia alle linee guida del WP sul consenso ai sensi del regolamento (UE) 2016/679, WP 259.01, 2018.

[327] Linee guida dell'EDPB n. 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19, p. 6.

[328] E. KOSTA, *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, Leiden, 2013, p. 251; L. CURREN, J. KAYE, *Revoking Consent: a "Blind Spot" in Data Protection Law?*, in *Comput. Law Secur. Rev.*, 2010, vol. 26, p. 273; C. BARTOLINI, L. SIRY, *The Right to be Forgotten in the Light of the Consent of the Data Subject*, in *Comput. Law Secur. Rev.*, 2016, vol. 32, p. 218. Sugli effetti che l'esercizio di questo diritto ha sulla ricerca

Di conseguenza, il titolare potrebbe essere costretto a interrompere l'attività di trattamento in corso e, se non può fare affidamento su un'altra base giuridica per conservare i dati per ulteriori trattamenti, a cancellare i dati [329].

L'esercizio del diritto di revoca può quindi mettere a rischio i risultati della ricerca basata sui dati ottenuti tramite il consenso [330]. In particolare, a essere compromessa è "*the representativeness and reliability of the research data, and thus [...] the integrity of research*" [331]. La scarsa rappresentatività nella ricerca può pregiudicare la generalizzabilità dei risultati e, così, la loro utilità per un ampio bacino di individui. Ad esempio, l'*American Society of Clinical Oncology* ha evidenziato che la scarsa diversificazione dei gruppi rappresentati nella ricerca oncologica fa sì che i risultati ottenuti non vadano a beneficio di chi ne ha più bisogno [332].

Di fronte a tali problematiche e nella prospettiva di assicurare il pieno conseguimento dei "veri" obiettivi del GDPR, sembra necessario superare una visione consenso-centrica e utilizzare le altre condizioni di liceità previste dalla normativa vigente, abbandonando l'idea secondo la quale queste debbano essere considerate come "eccezioni" alla regola generale del consenso [333]. Questo è particolarmente importante quando l'uso dei dati personali può portare a benefici significativi per la società [334], poiché la decisione del

---

biomedica, si rinvia a M. FLOREA, *Withdrawal of Consent for Processing Personal Data in Biomedical Research*, in *Int. Data Priv. Law*, 2023, vol. 13, n. 2, pp. 107-123.

[329] Artt. 17, par. 1, lett. b) e 3 GDPR. Occorre, tuttavia, ricordare che l'art. 17, par. 3, lett. d), GDPR prevede una deroga nel caso di trattamento dei dati a fini di ricerca scientifica, in conformità all'art. 89, par. 1, GDPR, qualora l'esercizio del diritto alla cancellazione "rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento". Cfr. linee guida dell'EDPB n. 05/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del regolamento (UE) 2016/679 (parte 1), versione 2.0, p. 12.

[330] E.S. DOVE, *op. cit*., 2018, p. 1023.

[331] Parere preliminare dell'EDPS sulla ricerca scientifica, 2020, p. 21. Anche E. VAYENA, A. BLASIMME, *op. cit.*, 2017, p. 509 sottolineano come la revoca del consenso mette a rischio "*the reliability and reproducibility of data analyses*".

[332] R.A. OYER et al., *Increasing Racial and Ethnic Diversity in Cancer Clinical Trials: An American Society of Clinical Oncology and Association of Community Cancer Centres Joint Research Statement*, in *J. Clin. Oncol.*, 2022, vol. 40, n. 19, pp. 2163-71.

[333] Come sembra invece emergere dalla sentenza *Meta Platforms e a*., dove la Corte ha stabilito che, in mancanza di consenso valido, le giustificazioni previste dalla norma devono essere interpretate restrittivamente (punti 91-93).

[334] È stato osservato come il consenso non rappresenti la base giuridica ottimale quando, ad esempio, "*societal benefits of data processing are compelling and risks to individuals are small*" (O. LYNSKEY, *op. cit.*, 2015, p. 246). Inoltre, come sottolineato recentemente dal CCNCE, il "paradigma di consenso rigidamente disegno-specifico" risulta essere inadeguato rispetto a metodologie di ricerca clinica e sanitaria innovative sia sperimentali che osservazionali (CCNCE, *op. cit*., 2023, pp. 16-17).

singolo di prestare o meno il proprio consenso alla raccolta e all'uso dei dati potrebbe non produrre "*the most desirable social outcome*" [335].

Infine, anche una volta superato questo approccio, le giustificazioni diverse dal consenso, che permettono di operare un bilanciamento (ad es. l'interesse pubblico [336] e l'interesse legittimo [337]), dovrebbero essere interpretate utilizzando il principio di proporzionalità secondo criteri il più possibile specifici.

Con riferimento alla base giuridica dell'interesse pubblico, possiamo trarre alcuni spunti utili dalla decisione della Corte in *Vyriausioji tarnybinės etikos komisija*, dove il principio di proporzionalità è stato applicato in tutte le tre componenti dell'idoneità, necessità e proporzionalità in senso stretto [338]. Dopo aver accertato che la misura nazionale era idonea a perseguire obiettivi di interesse generale riconosciuti dall'Unione *ex* art. 52, par. 1, Carta e di interesse pubblico *ex* art. 6, par. 3, GDPR, senza eccedere rispetto a quanto necessario per raggiungere tali obiettivi [339], la Corte ha

---

[335] D.J. SOLOVE, *op. cit*., 2013, p. 1881. Similmente, anche B.J. EVANS, *op. cit.*, 2011, p. 77 avverte riguardo al rischio che "*[a]n individual's wish not to participate, perhaps motivated by privacy concerns, potentially places other human beings at risk and undermines broader public interests – for example, in public health or medical discovery – in which the individual shares*".

[336] Art. 6, par. 1, lett. e), GDPR. Secondo l'Avvocato generale Pikamäe, questa condizione di liceità può essere utilizzata anche qualora il titolare del trattamento sia una persona giuridica di diritto privato (nel caso di specie, una società di valutazione del credito) che effettua un trattamento per fini di servizio pubblico. Ad esempio, nel settore della sanità pubblica, della protezione sociale e della gestione dei servizi di assistenza sanitaria (conclusioni dell'Avvocato generale Pikamäe del 16 marzo 2023, causa C-634/21, *Schufa Holding (Scoring)*, ECLI:EU:C:2023:220, punto 76). È tuttavia opportuno precisare che questa base giuridica, così come l'art. 6, par. 1, lett. c), GDPR, potrebbe non risultare la più adeguata nei casi di ricerca transfrontaliera. Infatti, ai sensi dell'art. 55, par. 2, GDPR, il meccanismo dello sportello unico non si applica ai trattamenti effettuati in virtù di un obbligo legale o per motivi di interesse pubblico, impedendo al titolare di avvalersi di un punto di contatto unico. Cfr. EDPS, *Study on the Secondary Use of Personal Data in the Context of Scientific Research*, Final Report EDPS/2019/02-04, p. 22.

[337] Art. 6, par. 1, lett. f), GDPR. Com'è noto, però, questa condizione di liceità è applicabile ai soli titolari del trattamento del settore privato e non anche alle autorità pubbliche (Art. 6, par. 1, e considerando 47 GDPR).

[338] Il medesimo approccio è stato adottato dalla Corte in *Commissione c. Polonia (Indipendenza e privacy dei giudici)* (punto 340) con riferimento alla base giuridica dell'art. 9, par. 2, lett. g), GDPR. In questo caso, la Corte ha riconosciuto che la raccolta e la pubblicazione online delle informazioni relative alla pregressa "iscrizione" di un giudice a un "partito politico" e alle "cariche" ricoperte in tale partito sono misure idonee a perseguire l'obiettivo di interesse pubblico di imparzialità dei giudici e di corretto esercizio della funzione giurisdizionale.

[339] Sentenza *Vyriausioji tarnybinės etikos komisija*, punto 83. Come ricordato nella sezione 2.1, nel caso di specie, la misura nazionale impone ai direttori di enti precettori di fondi

esaminato la possibilità di adottare misure alternative meno pregiudizievoli che permettessero di raggiungere i medesimi scopi di prevenzione dei conflitti di interessi e lotta alla corruzione [340] (ad es. limitando il numero di persone che possono consultare tali dati e il numero di informazioni condivise) [341].

La Corte ha poi rilevato la presenza di un'ingerenza grave nei diritti fondamentali di cui agli artt. 7 e 8 della Carta, a causa della natura dei dati trattati, della possibilità di combinare i dati per tracciare un ritratto dettagliato della vita delle persone interessate, nonché della natura delle modalità concrete del trattamento (ad es. il numero di persone che hanno accesso ai dati e le modalità di accesso) [342]. Nonostante questa ingerenza, è stato comunque effettuato un bilanciamento con gli obiettivi di interesse generale, verificando il soddisfacimento di determinati requisiti, tra cui la reale entità del fenomeno della corruzione all'interno del servizio pubblico del relativo Stato membro e la possibilità che l'interesse generale vari in base all'importanza delle funzioni svolte dal dichiarante, oltre alla presenza di benefici che compensino la gravità dell'ingerenza e di garanzie contro i rischi di abuso [343].

Un approccio interpretativo analogo dovrebbe essere adottato anche riguardo alla base giuridica dell'interesse legittimo, che fornisce "la necessaria flessibilità ai titolari del trattamento in situazioni in cui non sussiste un indebito impatto sugli interessati" [344]. Ciò implica, ad esempio, che – nell'applicare il test comparativo elaborato dal WP [345] – si debba tenere conto del fatto

---

pubblici di presentare una dichiarazione di interessi privati. Tale obbligo è volto a rafforzare le garanzie di probità e di imparzialità dei responsabili delle decisioni del settore pubblico, prevenire i conflitti di interessi e contrastare la corruzione nel servizio pubblico.

[340] *Ibid.* punto 88.

[341] *Ibid.* punti 93 e 96.

[342] *Ibid.* punti 99-102.

[343] *Ibid.* punti 111-113.

[344] Parere del WP n. 06/2014, p. 24.

[345] Questo test si fonda sulla verifica di "tre condizioni cumulative": i) il perseguimento dell'interesse legittimo del titolare del trattamento oppure del/i terzo/i a cui vengono comunicati i dati (ad es. l'esercizio della libertà di espressione e d'informazione, la prevenzione di frodi, la sicurezza informatica e il trattamento a scopi di ricerca); ii) la necessità del trattamento dei dati personali per il perseguimento dell'interesse legittimo, valutando la possibilità che vi siano altri mezzi meno invasivi per conseguire lo stesso obiettivo; iii) la condizione che non prevalgano i diritti e le libertà fondamentali della persona interessata, prendendo in considerazione la natura dei dati, le modalità di trattamento, le ragionevoli aspettative e lo status del responsabile del trattamento e dell'interessato (parere del WP n. 06/2014, p. 30 ss.). La Corte ha accolto il test comparativo, in diverse pronunce, tra cui la sentenza del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, ECLI:EU:C:2024:857, punti 37 ss.; del 7 dicembre 2023, causa C-634/21, *Schufa Holding*, ECLI:EU:C:2023:957; la sentenza *Meta Platforms e a*., punto 126; le sentenze del 15 giugno 2021, causa C-597/19, *M.I.C.M*, EU:C:2021:492, punto 106; del 29 luglio 2019, causa C-40/17, *Fashion ID*, ECLI:EU:C:2019:629,

che la "natura dell'interesse [del titolare del trattamento] può variare" [346]. In contesti simili a quelli della causa *Meta Platforms e a.*, il carattere economico e commerciale dell'interesse del titolare delle operazioni di trattamento difficilmente potrà considerarsi predominante rispetto all'interesse della società nel suo complesso. Tuttavia, si possono immaginare situazioni in cui l'interesse legittimo del titolare del trattamento (anche di natura economica) risulti preminente e vantaggioso per la società in generale, come – con adeguate garanzie – l'interesse della stampa a pubblicare informazioni sulla corruzione governativa o l'interesse a svolgere ricerca scientifica [347].

In tutti questi casi dove la protezione dei diritti e degli interessi del titolare non compromette quelli dell'interessato [348], dunque, il bilanciamento tra i vari diritti e interessi coinvolti dovrebbe considerare il fatto che l'operazione di trattamento non mira solo a soddisfare un interesse legittimo del titolare, ma anche un interesse pubblico. Pertanto, sarebbe opportuno attribuire maggiore rilevanza a quest'ultimo aspetto. In altre parole, come riconosciuto dallo stesso WP, "quanto più preminenti saranno l'interesse pubblico o l'interesse della collettività e quanto più la collettività e gli interessati si aspetteranno e riconosceranno chiaramente che il titolare del trattamento può intervenire e trattare i dati al fine di perseguire tali interessi, tanto maggiore sarà il peso di questo interesse legittimo nel bilanciamento" [349].

---

punto 95; la sentenza *Rīgas satiksme*, punto 28. Il test del WP è stato recentemente confermato dall'EDPB nelle *Guidelines n. 01/2024 on processing of personal data based on Article 6(1)(f)* e nell'*Opinion n. 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*. Infine, sulle incertezze e i rischi connessi all'utilizzo della base giuridica dell'interesse legittimo, cfr. F. FERRETTI, *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?*, in *CMLRev*., 2014, n. 3, p. 843.

[346] Parere del WP n. 06/2014, p. 29.

[347] *Ibid.* Ulteriori esempi vengono forniti a p. 41: "un ente di beneficenza o un'associazione senza scopo di lucro potrebbero trattare dati personali rispettivamente a fini di ricerca medica e di sensibilizzazione sulla corruzione governativa. Può anche succedere che l'interesse imprenditoriale privato di un'azienda coincida in qualche misura con un interesse pubblico. Questa situazione potrebbe verificarsi, per esempio, nel caso della lotta alle frodi finanziarie o ad altri usi fraudolenti dei servizi. Un fornitore di servizi può avere un interesse imprenditoriale legittimo a garantire che i suoi clienti non utilizzino il servizio in maniera impropria (o che non possano ottenere i servizi senza aver pagato per fruirne) e, al tempo stesso, i clienti dell'impresa, i contribuenti e il pubblico in generale hanno a loro volta un interesse legittimo a garantire che le attività fraudolente siano scoraggiate e individuate quando si verificano".

[348] P. BRAVO, *op. cit*., 2018, p. 31.

[349] Parere n. 06/2014, p. 42, in cui si afferma anche che, in caso di mancato trattamento, è necessario valutare l'eventuale danno subìto dal titolare, da terzi e dalla collettività. Tuttavia, ciò non consente di far coincidere l'interesse pubblico (art. 6, par. 1, lett. e), GDPR) con l'interesse legittimo (art. 6, par. 1, lett. f), GDPR), che restano condizioni autonome e distinte di liceità di trattamento, anche qualora gli interessi perseguiti dal titolare possano concorrere alla

4. Riflessioni conclusive

Il *favor* per la tutela dei diritti personalistici degli individui rispetto alle operazioni di trattamento dei dati ha ragioni storiche profonde, che comprendono il legame del diritto alla protezione dei dati personali con il diritto alla riservatezza, oltre alla necessità di superare la logica economica che aveva permesso al legislatore europeo del 1995 di intervenire a difesa dei diritti e delle libertà fondamentali delle persone fisiche. Pertanto, orientamenti interpretativi come quelli consolidatisi sino ad ora in merito al GDPR, se collocati in un contesto caratterizzato dall'esigenza di offrire una protezione effettiva agli individui contro trattamenti illeciti di dati, non sollevano particolari obiezioni. Tuttavia, in un contesto storico e normativo profondamente mutato, nel quale è ormai evidente che alcuni trattamenti di dati personali possono generare benefici significativi per la collettività, l'adozione di questa chiave interpretativa nella lettura non solo dello EHDS e degli altri regolamenti della Strategia europea per i dati, ma anche delle norme del GDPR, rischia di pregiudicare la realizzazione degli obiettivi perseguiti.

Per sfuggire a una simile eventualità, in questo capitolo si è proposto un approccio interpretativo alternativo volto a riflettere più fedelmente le scelte legislative compiute con lo EHDS e il GDPR. In particolare, attraverso un ridimensionamento della portata applicativa del GDPR e un utilizzo sistematico del principio di proporzionalità, riteniamo si possa raggiungere un equilibrio adeguato tra la protezione degli interessati e dei titolari del trattamento, in quanto portatori di interessi individuali e collettivi. Come osservato infatti dall'Avvocato generale Pitruzzella nella causa *Ligue des droits humains*, la barriera eretta dal costituzionalismo europeo a tutela dell'individuo e delle sue libertà non dovrebbe pregiudicare taluni interessi fondamentali della società (ad es. la protezione della sanità pubblica, la sostenibilità ambientale, la lotta contro il terrorismo e la prevenzione dei reati) che a loro volta possono avere legami costituzionali [350].

---

realizzazione di finalità di rilevanza collettiva. A tale proposito, le linee guida n. 01/2024 dell'EDPB hanno chiarito che: "*[t]he interests of the wider community are mainly subject to the justifications provided for in Article 6(1)(e) or (c), if controllers are tasked or required by law to preserve or pursue such interests. This is the case, for instance, when private operators are obliged to assist law enforcement authorities in their efforts to combat certain illegal activities. Where a controller carries out further activities which do not fall within such specific legal obligations set out in laws and regulations, it needs to demonstrate that this is done in pursuit of the controller's own legitimate interests or those of specific third parties. In any event, a legitimate interest may not be invoked with the aim or effect of circumventing legal requirements*" (EDPB, *Guidelines n. 01/2024 on processing of personal data based on Article 6(1)(f) GDPR*, punto 25).

[350] Conclusioni dell'Avvocato generale Pitruzzella in *Ligue des droits humains*, p. 2. In

In questa prospettiva, le alternative interpretative suggerite con la presente analisi in riferimento al GDPR potrebbero avere diversi risvolti positivi. In primo luogo, contribuire all'effettività del GDPR, garantendo che le sue disposizioni producano pienamente i loro effetti e raggiungano il loro scopo [351]. In secondo luogo, favorire una maggiore coerenza nell'ordinamento giuridico europeo, specialmente rispetto agli obiettivi perseguiti dagli atti adottati nell'ambito della Strategia europea per i dati. A tal fine, un ruolo centrale spetta alle istituzioni europee, le quali, in uno spirito di leale cooperazione [352], sono tenute a garantire la coerenza dell'ordinamento giuridico dell'Unione [353], affinché le diverse parti che lo compongono "*hang together and make sense as a whole*" [354].

una causa riguardante, *inter alia*, la validità della direttiva (UE) 2016/681, l'Avvocato generale ha colto l'occasione per svolgere alcune considerazioni di carattere generale sulle potenzialità (ad es. la lotta al terrorismo) e i rischi (ad es. la sorveglianza di massa) legati all'uso di tecnologie digitali, come l'Intelligenza Artificiale, per conservare e trattare grandi quantità di dati (nel caso di specie, i dati del codice di prenotazione).

[351] Sul principio di effettività nell'ordinamento giuridico europeo, si rinvia, *ex multis*, a I. INGRAVALLO, *L'effetto utile nell'interpretazione del diritto dell'Unione europea*, Cacucci, Bari, 2017; M. ROSS, *Effectiveness in the European Legal Order(s): Beyond Supremacy to Constitutional Proportionality?*, in *Eur. Law Rev.*, 2006, vol. 4, p. 480; M. ACETTO, S. ZLEPTING, *The Principle of Effectiveness: Rethinking Its Role in Community Law*, in *Eur. Pub. L.*, 2005, vol. 11, p. 375.

[352] Art. 4, par. 3, TUE. Cfr., *inter alia*, F. CASOLARI, *Leale cooperazione tra Stati membri e Unione Europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Editoriale scientifica, Napoli, 2020; M. KLAMERT, *The Principle of Loyalty in EU Law*, OUP, Oxford, 2014.

[353] Art. 13, par. 2, TUE.

[354] J. BENGOETXEA, N. MACCORMICK, L.M. SORIANO, *Integration and Integrity in the Legal Reasoning of the European Court of Justice*, in G. DE BÚRCA, J.H.H. WEILER (eds.), *The European Court of Justice*, OUP, Oxford, 2001, p. 47.

Capitolo 4
Il GDPR alla prova dello spazio europeo dei dati sanitari: nuovi scenari applicativi

"*Effettuare il bilanciamento non significa semplicemente trovare un compromesso, ma piuttosto operare scelte di ordine costituzionale in un ordinamento composito, cercando di pervenire a soluzioni armoniose, che trovino il giusto equilibrio fra regole europee e istanze nazionali [...] Queste scelte delicate [...] contribuiranno nel tempo a forgiare l'identità europea*".

(Rossi, 2024) [1]

Sommario: 1. Premessa. – 2. Gli ostacoli alla libera circolazione dei dati personali nel GDPR: Italia e Francia a confronto. – 2.1. La frammentazione normativa. – 2.1.1. Il Codice della privacy italiano e alcuni cenni (preliminari) al Fascicolo Sanitario Elettronico. – 2.1.2. La legge francese sulla protezione dei dati e il sistema centralizzato dell'*Health Data Hub*. – 2.1.3. L'imperfetta coincidenza tra le disposizioni nazionali e i possibili effetti sulla libera circolazione dei dati. – 2.2. La disomogeneità delle prassi amministrative. – 2.2.1. Il Garante per la protezione dei dati personali e la tutela della persona. – 2.2.2. La *Commission Nationale de l'Informatique et des Libertés* e le occasioni per la ricerca. – 2.2.3. Gli elementi di differenziazione tra le prassi amministrative delle autorità di controllo e i correttivi presenti nel GDPR. – 3. Verso un'applicazione del GDPR maggiormente uniforme alla luce delle novità introdotte dallo spazio europeo dei dati sanitari. – 3.1. Alcune ipotesi di revisione del testo del GDPR. – 3.1.1. Una definizione comune di "ricerca scientifica". – 3.1.2. Le misure di garanzia e il margine di manovra degli Stati membri. – 3.2. La verifica della compatibilità del diritto nazionale di applicazione del GDPR con il diritto dell'Unione. – 3.2.1. (*Segue*) Nelle ipotesi di trattamento puramente "interne". – 3.2.2. (*Segue*) Nelle ipotesi di trattamento a carattere transfrontaliero. – 4. Riflessioni conclusive.

1. Premessa

Al termine del capitolo precedente abbiamo esaminato le potenziali tensioni tra il regolamento sullo EHDS e il GDPR, specialmente se quest'ultimo

[1] L.S. Rossi, *Il principio del primato come "regola di coesione" dell'ordinamento dell'Unione europea*, in *Quaderni AISDUE*, 2024, fasc. 1, p. 18.

continua a essere interpretato in modo tale da privilegiare la protezione dei diritti degli interessati a scapito di altri diritti e interessi meritevoli di tutela. In questo capitolo, invece, ci soffermeremo sulle tensioni che possono emergere tra queste due discipline nel caso in cui l'applicazione del GDPR, e in particolare di alcune delle sue disposizioni, resti estremamente disomogenea tra gli Stati membri [2]. Come vedremo in seguito, questa situazione ostacola la libera circolazione dei dati personali nell'Unione, la quale rappresenta un obiettivo perseguito dalla normativa europea sui dati personali e non personali, attualmente anche in ambito sanitario.

Sin dai primi tentativi di regolazione del mondo digitale e delle sfide ad esso connesse, il legislatore europeo ha aspirato al raggiungimento di un felice connubio tra la protezione e la libera circolazione dei dati all'interno dell'Unione. In particolare, la crescente consapevolezza del contributo che l'affermarsi di quest'ultima avrebbe comportato al fiorire del mercato unico digitale [3] ha condotto e giustificato l'adozione del GDPR e del successivo regolamento sulla libera circolazione dei dati non personali (FFR) [4]. Questi strumenti normativi – oggi affiancati da un *corpus* sempre più ampio di nuovi atti, tra cui lo EHDS [5] – sono stati concepiti per creare un insieme coerente di norme, capace di superare gli ostacoli tecnici e normativi al flusso dei dati tra gli Stati membri [6].

---

[2] Cfr. Risoluzione del Parlamento europeo del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP)), p. 4.

[3] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Strategia per il mercato unico digitale in Europa, COM(2015) 192 final, del 6 maggio 2015.

[4] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (FFR), in cui viene sancito lo stesso principio di libera circolazione dei dati che stabilisce il GDPR, ma in riferimento ai dati non personali. Con tale regolamento, al fine di favorire lo scambio dei dati non personali nel mondo digitale, il legislatore europeo ha previsto obblighi di localizzazione dei dati, la messa a disposizione di dati alle autorità di controllo e la portabilità degli stessi per gli utenti professionali.

[5] Basti pensare ai regolamenti adottati nell'ambito della Strategia europea dei dati del 2020 (COM(2020) 66 final, del 19 febbraio 2020), come il 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 (DGA), che completa quanto disposto nella direttiva 2019/1024 (direttiva *open data*), il regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (DA).

[6] COM(2015) 192 final, p. 16. Anche se la base giuridica del GDPR (art. 16, par. 2, TFUE) e del FFR (art. 114 TFUE) possa far pensare che, nel primo dei due strumenti normativi, il diritto alla protezione dei dati sia preminente rispetto alla libera circolazione di questi ultimi,

Concentrandosi sui dati personali, è opportuno ricordare che l'intervento comunitario in questo campo fu originariamente motivato dalla necessità di far fronte all'aumento dell'uso dei dati personali "in tutti gli aspetti delle attività economiche e sociali" e alle "nuove esigenze in materia di scambio di dati" [7]. Le preoccupazioni per l'assenza di una disciplina comune o per l'adozione di approcci normativi nazionali divergenti, espresse con forza dal Parlamento europeo [8], spinsero la Commissione a proporre un atto focalizzato unicamente sulla protezione delle persone in relazione al trattamento dei dati personali. Come noto, tuttavia, al momento della proposta, l'Unione non disponeva di alcuna competenza per adottare una disciplina in materia di diritti fondamentali [9].

---

come vedremo, anche nel GDPR il principio di libera circolazione dei dati rappresenta una caratteristica essenziale. Si anticipi sin da ora che la stessa Commissione, con riferimento alle ipotesi in cui gli Stati possono disciplinare materie specifiche (ad es. la ricerca scientifica), evidenzia come questi "dovrebbero essere incoraggiati a non fare uso delle clausole di deroga del regolamento per limitare ulteriormente la libera circolazione dei dati". Cfr. Comunicazione della Commissione, Costruire un'economia dei dati europea, COM(2017) 9 final, del 10 gennaio 2017, pp. 5-8. Sul rapporto tra il GDPR e il FFR, F. FERRI, *Il bilanciamento tra diritti fondamentali nel mercato unico digitale*, Giappichelli, Torino, 2022, p. 313 ss.: l'A. osserva come la differenza più rilevante tra le due normative consista nel fatto che il GDPR si fonda "sull'esigenza di salvaguardare il diritto fondamentale alla protezione dei dati personali, conciliandolo con altri diritti riconosciuti e garantiti dalla Carta", mentre il FFR "ha un'anima decisamente più mercantilistica".

[7] Comunicazione della Commissione concernente la protezione delle persone per quanto riguarda il trattamento dei dati personali nella Comunità e la sicurezza dei sistemi d'informazione, COM(1990)314, del 13 settembre 1990, p. 2.

[8] *Ibid.* p. 3. Con Lisbona e l'acquisizione del ruolo di co-legislatore, il Parlamento ha potuto esercitare una maggiore influenza sulla formulazione del GDPR, contribuendo all'adozione di un approccio caratterizzato da una "*strong emphasis on fundamental rights*" (T. STREINZ, *The Evolution of European Data Law*, in P. CRAIG, G. DE BÚRCA (eds.), *The Evolution of EU Law*, OUP, Oxford, 2021, p. 909).

[9] Parere della Corte 2/94 del 28 marzo 1998, ECLI:EU:C:1996:140, punto 27. Per un approfondimento dottrinale sulle competenze dell'Unione in materia di diritti fondamentali, si rinvia, *ex multis*, L.S. ROSSI (a cura di), *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, Giuffrè, Milano, 2002; G. STROZZI, *Il sistema integrato di tutela dei diritti fondamentali dopo Lisbona: attualità e prospettive*, in L.F. PACE (a cura di), *Nuove tendenze del diritto dell'Unione europea dopo il Trattato di Lisbona*, Giuffrè, Milano, 2012, p. 33 ss.; A. PERTICI, *Dall'Europa dei mercati all'Europa dei diritti*, in G. RIVOSECCHI, M. ZUPPETTA (a cura di), *Governo dell'economia e diritti fondamentali dell'Unione europea*, Cacucci, Bari, 2010, pp. 79-102; L. TRUCCO, *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione Europea. Un'analisi delle strategie argomentative e delle tecniche decisorie a Lussemburgo*, Giappichelli, Torino, 2013, pp. 128-129; N. NAPOLETANO, *L'evoluzione della tutela dei diritti fondamentali nell'Unione europea*, in A. CALIGURI, G. CATALDI, N. NAPOLETANO (a cura di), *La tutela dei diritti umani in Europa: tra sovranità statale e ordinamenti sovranazionali*, Cedam, Padova, 2010, pp. 3-50; S. DOUGLAS-SCOTT, *The European Union and Human Rights after the Treaty of Lisbon*, in *HRLRev*., 2011, vol. 11, n. 4, pp. 645-682.

Per questo motivo, nonostante le resistenze della Commissione, il Consiglio insistette affinché tra gli obiettivi della direttiva madre (DPD) fosse incluso anche il riferimento alla libera circolazione dei dati personali [10], sottolineando come quest'ultima fosse finalizzata a stabilire un "*working single market*" [11]. Questa precisazione ha permesso di giustificare l'adozione della DPD sulla base dell'art. 100A TCE (oggi, art. 114 TFUE). Solo prevedendo "una protezione equivalente di elevato livello in tutti gli Stati Membri" sarebbe stato possibile rimuovere gli ostacoli allo scambio dei dati personali, evitando che l'adozione di normative nazionali eterogenee e concorrenti compromettesse la realizzazione effettiva delle libertà fondamentali del mercato interno [12].

La DPD nacque dunque come misura di natura essenzialmente economica [13], in cui la finalità di tutelare il diritto fondamentale degli individui alla protezione dei dati personali era funzionale rispetto all'armonizzazione del mercato interno [14]. Diversamente, con il GDPR, gli obiettivi di "assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione" [15] assumono, almeno formalmente, un'importanza paritaria. D'altronde è lo stesso art. 16, par. 2, TFUE – su cui il GDPR si fonda – ad affermare congiuntamente la protezione delle persone fisiche riguardo al

---

[10] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[11] Proposta modificata di direttiva del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, COM(92) 422 final, del 15 ottobre 1992, p. 8.

[12] Considerando 3 DPD.

[13] Sull'iter che ha portato all'adozione della DPD, si rinvia a H. HEIL, *Directive 95/46/EC of the European Parliament and the Council*, in A. BÜLLESBACH, Y. POULLET, C. PRINS (eds.), *Concise European IT Law*, Kluwer Law International, Alphen aan den Rijn, 2010, p. 11; S. SIMITIS, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, in *Iowa L. Rev.*, 1995, vol. 80, p. 449.

[14] Ciò non toglie che nella DPD, accanto alla dimensione economica, vi fosse anche una dimensione legata ai diritti fondamentali e, in particolare, all'art. 8 della Carta (prima relazione della Commissione sulla direttiva 95/46/CE sulla protezione dei dati personali, COM(2003) 265 final, del 15 maggio 2003, p. 4). Quest'ultima emerge chiaramente da alcune scelte operate dal legislatore (ad es. la possibilità di condividere i dati relativi alla salute viene ammessa come eccezione e non come regola) ed è destinata ad avere un impatto sull'interpretazione della direttiva ad opera della Corte. Cfr. T. HERVEY, J. MCHALE, *Data Protection and Health Information Privacy*, in T. HERVEY, J. MCHALE, *Health Law and the European Union*, CUP, Cambridge, 2004, p. 167; T. STREINZ, *op. cit.*, 2021, p. 910.

[15] Considerando 10 GDPR, da leggere in combinato disposto con il considerando 13 e l'art. 1 GDPR.

trattamento dei loro dati e l'esigenza di garantire l'utilizzo e la libera circolazione degli stessi nell'Unione [16].

Tuttavia, nel leggere tale disposizione e, di riflesso, l'intero GDPR, l'enfasi viene tipicamente posta sulla prima componente, probabilmente per via del richiamo esplicito nel primo paragrafo dell'art. 16 TFUE al diritto fondamentale alla protezione dei dati personali. Come anticipato nel capitolo 3, questo tipo di approccio interpretativo sta subendo, alla luce del mutato contesto storico e normativo, uno stress test circa la sua capacità di coniugare in modo adeguato la protezione degli interessati riguardo al trattamento dei loro dati e la valorizzazione del potenziale derivante dall'uso e dalla condivisione degli stessi, anche a livello transfrontaliero. Questo scenario è particolarmente evidente nelle situazioni in cui ci si confronta con uno dei principali dilemmi del costituzionalismo liberal-democratico: il bilanciamento tra i diritti individuali (di controllo) sui dati e l'interesse della collettività a utilizzarli [17].

---

[16] Con il Trattato di Lisbona, concepito per gettare "una nuova luce sui diritti degli individui in quanto cittadini dell'Unione" (Comunicazione della Commissione al Consiglio, La revisione dell'Europa per il XXI secolo, COM(2007) 412 final, del 10 luglio 2007, p. 7), l'art. 16, par. 2, TFUE viene introdotto come base giuridica per la materia della protezione e circolazione dei dati personali, salvo per quelli rientranti nelle materie di politica estera e sicurezza comune, andando a sostituire il precedente art. 286 TCE, introdotto dal Trattato di Amsterdam per rafforzare i "diritti fondamentali come applicazione del diritto della persona alla tutela della riservatezza" (F. POCAR, M.C. BARUFFI, A. ADINOLFI, *Commentario breve ai Trattati dell'Unione europea*, Cedam, Assago, 2014, p. 189). Sul punto, in dottrina, cfr. G. ZANFRINFORTUNA, *Article 16 TFEU – Commentary*, in H-J. BLANKE, S. MANGIAMELI (eds.), *The Treaty on the Functioning of the European Union. A Commentary*, Springer, Berlin, 2021; H. HIJMANS, *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*, Springer, Berlin, 2016; M. KELLERBAUER, M. KLAMER, J. TOMKIN (eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, OUP, Oxford, 2019, p. 406; O. LYNSKEY, *The Foundations of EU Data Protection Law*, OUP, Oxford, 2015, p. 58.

[17] Espressione tratta dalle conclusioni dell'Avvocato generale Pitruzzella in una causa relativa all'interpretazione del GDPR e alla validità della direttiva sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Tra le considerazioni preliminari effettuate, viene sottolineato come le questioni sottoposte all'attenzione della Corte rientrino "nell'ambito di uno dei principali dilemmi del costituzionalismo liberale democratico contemporaneo: come debba essere definito l'equilibrio fra l'individuo e la collettività nell'era dei dati, quando le tecnologie digitali hanno consentito la raccolta, la conservazione, il trattamento e l'analisi di enormi masse di dati personali a fini predittivi. Gli algoritmi, l'analisi dei big data e l'intelligenza artificiale utilizzati dalle autorità pubbliche possono servire a promuovere e a proteggere gli interessi fondamentali della società, con un'efficacia in precedenza inimmaginabile: dalla protezione della sanità pubblica alla sostenibilità ambientale, dalla lotta contro il terrorismo alla prevenzione dei reati, in particolare dei reati gravi. Allo stesso tempo, la raccolta indiscriminata di dati personali e l'utilizzazione delle tecnologie digitali da parte dei poteri pubblici possono dare luogo ad un panottico digitale, vale a dire ad un potere pubblico che vede senza essere visto. […] Come è noto, in taluni paesi la società prevale sull'individuo e

Un equilibrio che si rivela ancora più difficile da raggiungere in settori come quello sanitario, dove l'interesse all'uso dei dati permette di ottimizzare i servizi sanitari e di promuovere il progresso scientifico in questo ambito, offrendo vantaggi sia per l'individuo sia per la collettività. Nel contesto attuale di crescente digitalizzazione, che investe in modo significativo settori cruciali come la sanità e la ricerca scientifica, riuscire a conciliare le suddette istanze appare quanto mai centrale. Oggi, ad esempio, le attività di ricerca non possono prescindere dall'uso e dalla condivisione di un numero massiccio di dati (i c.d. *Big Data*) [18], il cui carattere di non rivalità fa sì che il loro valore aumenti in modo direttamente proporzionato alla possibilità che questi vengano utilizzati e condivisi [19].

In quest'ottica, come insegna la letteratura economica, non sarebbe collettivamente efficiente imporre diritti individuali troppo stringenti [20]. Inoltre, dal

---

l'utilizzazione dei dati personali consente legittimamente di realizzare una sorveglianza di massa efficace volta a proteggere interessi pubblici considerati fondamentali. Viceversa, il costituzionalismo europeo – nazionale e sovranazionale – il quale assegna un posto centrale all'individuo e alle sue libertà, mette una barriera importante all'avvento di una società della sorveglianza di massa, soprattutto dopo il riconoscimento dei diritti fondamentali alla protezione della vita privata e alla protezione dei dati personali. Si pone tuttavia la questione della misura in cui tale barriera possa essere eretta senza arrecare un grave pregiudizio a taluni interessi fondamentali della società – come quelli citati in precedenza a titolo esemplificativo – i quali possono tuttavia avere legami costituzionali. Ci si trova al cuore della questione del rapporto fra individuo e collettività nella società digitale. Una questione che esige, da un lato, la ricerca e l'attuazione di equilibri delicati fra gli interessi della collettività e i diritti degli individui, prendendo le mosse dall'importanza assoluta che questi ultimi hanno nel patrimonio costituzionale europeo, e, dall'altro, la predisposizione di garanzie contro gli abusi" (conclusioni dell'Avvocato generale Pitruzzella del 27 gennaio 2022, *Ligue des droits humains*, ECLI:EU:C:2022:65, pp. 2 e 3).

[18] In letteratura è stato rilevato il passaggio da un approccio teoria-centrico, dove "l'utilità dei dati sta nel funzionare come prova della plausibilità di una ipotesi già data, confermando così asserzioni che i ricercatori interpretano come nuove scoperte", a un approccio dato-centrico, in cui "i dati sono visti come entità pubbliche che hanno valore scientifico indipendentemente dal loro ruolo di prova per una determinata ipotesi e che possono essere interpretato in modi diversi a seconda delle abilità e degli interessi dei ricercatori che li analizzano" (S. LEONELLI, *La ricerca scientifica nell'era dei big data. Cinque modi in cui i Big Data danneggiano la scienza, e come salvarla*, Meltemi, Milano, 2018, pp. 28-29). Sul punto, si rinvia anche all'analisi di P. QUINN, *Research Under The GDPR – A Level Playing Field for Public and Private Sector Research*, in *Life Sci. Soc. Policy*, 2021, vol. 17, n. 4, p. 28.

[19] Y. CARRIÈRE-SWALLOW, V. HAKSAR, *International Monetary Fund; Issuing Body. The Economics and Implications of Data: An Integrated Perspective*, in *IMF*, 2019, p. 14, in cui gli A. evidenziano come "*[a]n important implication of the nonrivalry of data is that, from a social perspective, it is desirable for data to be widely shared*".

[20] Tra gli studiosi di *law and economics*, si registra un generale consenso nel ritenere che "*more information is better, and restrictions on the flow of information in the name of privacy are generally not social wealth maximizing, because they inhibit decision making, increase*

momento che "*[r]esearchers, particularly in medical research, often work in large collaborative networks and need to exchange large volumes of data at great speed across border*" [21], assicurare la mobilità dei dati personali tra gli Stati membri, specialmente in alcuni settori, come quello sanitario, rappresenta un fattore abilitante non solo per il prosperare del mercato unico digitale, ma anche per l'effettivo godimento di diritti fondamentali, come il diritto alla salute, e per il rispetto dei principi del Pilastro europeo dei diritti sociali, tra cui l'accesso equo a servizi sanitari.

Di fronte a questo tipo di esigenze, appare necessario interrogarsi non solo sull'interpretazione del GDPR, come è stato fatto nel capitolo precedente, ma anche sul suo attuale stato di applicazione a livello nazionale. Pertanto, nelle pagine che seguono descriveremo la situazione di frammentazione normativa derivante dalla scelta del legislatore del 2016 di deferire agli interpreti nazionali l'operazione di bilanciamento tra il diritto individuale alla protezione dei dati personali, gli interessi dei titolari del trattamento e dei terzi, nonché l'eventuale interesse pubblico a trattare i suddetti dati. Lo scopo di questa analisi è evidenziare come tale situazione rischi di rappresentare un ostacolo a uno degli obiettivi del GDPR, ossia la libera circolazione dei dati personali [22], perseguito oggi, seppur in ambito sanitario, dallo EHDS (sezione 2). In questo modo, a ben vedere, potrebbe risultare compromesso anche il futuro dello EHDS, con il quale sono state compiute delle scelte che si ritiene debbano offrire nuovi criteri di lettura rispetto a quelli adottati con il GDPR e con le norme nazionali di applicazione dello stesso, aprendo prospettive di revisione del quadro normativo esistente (sezione 3).

2. Gli ostacoli alla libera circolazione dei dati personali nel GDPR: Italia e Francia a confronto

Dal 2018, anno dell'entrata in vigore del GDPR, fino ad oggi, appare quantomai evidente la mancanza di effettività di questo strumento normativo, se

transactions costs, and encourage fraud" (R.S. MURPHY, *Property Rights in Personal Information: An Economic Defense of Privacy*, in *Geo. L. J.*, 1996, vol. 84, p. 2382).

[21] EDPS, *A Preliminary Opinion on Data Protection and Scientific Research*, 2020, p. 6.

[22] La presente analisi non affronta in modo specifico altri fattori che possono costituire un ostacolo alla libera circolazione dei dati personali, come la mancanza di interoperabilità tecnica e semantica, né si sofferma su quelli che limitano lo scambio di dati non personali. Per un approfondimento su quest'ultimo aspetto, si rinvia a O. BATURA et al., *The Emergence of Non-Personal Data Markets*, Publication for the Committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2023, pp. 50-55.

non altro per quanto riguarda l'obiettivo di garantire la libera circolazione dei dati personali all'interno dell'Unione tramite l'adozione di regole direttamente applicabili in tutti gli Stati membri [23]. L'assenza di un consenso ampio rispetto alla definizione del livello di protezione da assicurare ai soggetti coinvolti nelle attività di trattamento dei dati personali ha, infatti, limitato, se non addirittura precluso, la possibilità di fissare un "tetto comune" in questo settore [24], creando una situazione di estrema frammentazione normativa [25] e applicativa della disciplina in questione.

In primo luogo, nonostante la natura formale di regolamento [26], è ormai noto che il GDPR lascia un margine di discrezionalità ai legislatori nazionali, specialmente per quanto riguarda i trattamenti di dati sanitari per finalità di ricerca scientifica, molto maggiore rispetto a quello concesso dalla DPD che, come affermato dalla Corte, non mirava a un'armonizzazione minima, ma in linea di principio completa [27] (sezione 2.1). In secondo luogo, si osserva una certa disomogeneità nelle prassi amministrative delle autorità di controllo, le quali invece dovrebbero garantire un'applicazione coerente del GDPR per la protezione delle persone fisiche in relazione al trattamento dei loro dati e facilitare la libera circolazione degli stessi nel mercato interno (sezione 2.2).

---

[23] Art. 1, par. 3, e considerando 10 GDPR.

[24] O. POLLICINO, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 2023, fasc. 3, p. 584.

[25] Per un quadro generale sulle principali differenze tra le discipline nazionali rilevate in questo specifico ambito, cfr. DG SANTE, *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, 2021.

[26] Come noto, ai sensi dell'art. 288 TFUE, il regolamento "è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri", diversamente dalle direttive che, invece, vincolano gli Stati "quanto al risultato da raggiungere, lasciando alle autorità nazionali la scelta della forma e dei mezzi". Sulla scelta dello strumento normativo del regolamento per il GDPR, v. considerando 9 GDPR e relazione della Commissione alla proposta di regolamento, in cui si afferma che "il Regolamento è considerato lo strumento più idoneo per definire il quadro giuridico per la protezione dei dati personali nell'UE. L'applicabilità diretta di un Regolamento ai sensi dell'art. 288 TFUE ridurrà la frammentazione giuridica e offrirà maggiore certezza giuridica grazie all'introduzione di una serie di norme di base armonizzate, migliorando la tutela dei diritti fondamentali delle persone fisiche e contribuendo al corretto funzionamento del mercato interno".

[27] Sentenze della Corte del 29 luglio 2019, causa C-40/17, *Fashion ID*, ECLI:EU:C:2019:629, punto 54; del 24 novembre 2011, cause riunite C-468/10 e C-469/10, *ASNEF*, ECLI:EU:C:2011:777, punto 29; del 6 novembre 2003, causa C-101/01, *Lindqvist*, ECLI:EU:C:2003:596, punto 96.

2.1. La frammentazione normativa

Il mancato superamento della situazione di frammentazione normativa, risultante dagli anni di interpretazione e applicazione della DPD [28], è stato da tempo considerato uno dei principali indicatori del fallimento del GDPR rispetto alla realizzazione della libera circolazione dei dati personali nell'Unione [29]. Nel lungo e travagliato processo di negoziazione che ha portato all'adozione del GDPR, infatti, la volontà politico-istituzionale [30] fu quella di evitare di giungere a soluzioni di compromesso su aspetti che, sollevando questioni di portata costituzionale [31], si preferì lasciare agli Stati membri affinché

[28] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Salvaguardare la privacy in un mondo interconnesso Un quadro europeo della protezione dei dati per il XXI secolo, COM(2012) 9 final, del 25 gennaio 2012, p. 7: "[b]enché l'attuale direttiva si prefigga di garantire un livello equivalente di protezione dei dati in tutta l'Unione, tra i vari Stati membri persistono notevoli differenze quanto a norme applicate. Di conseguenza, i responsabili del trattamento possono trovarsi di fronte a 27 legislazioni e requisiti nazionali diversi all'interno dell'Unione. Ne risulta un quadro normativo frammentato, che genera incertezza giuridica e porta a una protezione diseguale delle persone fisiche. Tale situazione produce costi inutili e oneri amministrativi per le imprese e disincentiva le imprese che operano nel mercato interno dall'espandere le loro attività all'estero. Le risorse e i poteri delle autorità nazionali di protezione dei dati variano sensibilmente da uno Stato membro all'altro. In alcuni casi ciò significa che tali autorità non sono in grado di esercitare i compiti di controllo in modo soddisfacente. La cooperazione tra le autorità nazionali di protezione dei dati a livello europeo – attraverso l'attuale gruppo consultivo (gruppo di lavoro "articolo 29") – non garantisce sempre un'applicazione coerente della normativa e pertanto occorre migliorarla".

[29] Sebbene nelle relazioni di valutazione sull'applicazione del GDPR le istituzioni riconoscano il successo del GDPR nel conseguire i suoi obiettivi, non mancano osservazioni critiche sugli effetti negativi che la frammentazione normativa produce sulla libera circolazione dei dati personali. Si veda, in particolare, la Comunicazione della Commissione al Parlamento europeo e al Consiglio, Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati, COM(2024) 357 final, del 25 luglio 2024, p. 9; Comunicazione della Commissione al Parlamento europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, COM(2020) 264 final, del 24 giugno 2020, p. 7; la Risoluzione del Parlamento europeo sulla relazione di valutazione della Commissione; la posizione del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (regolamento generale sulla protezione dei dati) (14994/2/19 REV 2), del 15 gennaio 2020, p. 11.

[30] Nella posizione del Consiglio sull'attuazione del GDPR viene spiegato come la decisione di lasciare un margine di manovra agli Stati membri per mantenere o introdurre disposizioni più specifiche è stata "intenzionale" per consentire la precisazione di alcune disposizioni del GDPR e che, quindi, una certa frammentazione è giustificata (p. 16).

[31] Come abbiamo visto nel capitolo 1 (sezione 2.2, nota 88), all'interno dell'ordinamento giuridico europeo, sia la tutela della salute umana sia la ricerca e lo sviluppo tecnologico rappresentano una prerogativa nazionale. Di conseguenza, il margine di discrezionalità degli Stati

fossero questi a conciliare i diritti e gli interessi in gioco nel rispetto dei principi di sussidiarietà e proporzionalità [32].

Ne è risultato un testo costellato di clausole di apertura facoltative, che offrono la possibilità agli Stati membri di introdurre norme nazionali supplementari, più rigorose o a carattere derogatorio [33]. Sono proprio queste clausole di apertura a fare in modo che l'armonizzazione operata dal GDPR vari "a seconda delle disposizioni considerate" [34], rendendo tale strumento normativo del tutto peculiare rispetto a un classico regolamento e avvicinandolo piuttosto a una direttiva ("direttiva mascherata") [35]. Basti pensare alle disposizioni relative alla base giuridica dell'attività di trattamento [36], alla portata dei diritti

può essere inteso quale corollario del riparto di competenze stabilito dai Trattati. Cfr. G. DI FEDERICO, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in E. AL MUREDEN, C. BOTTARI (eds.), *La salute del futuro: prospettive e nuove sfide del diritto sanitario*, Bononia University Press, Bologna, 2020, p. 35 e F. MOLNÁR-GÁBOR et al., *Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome Them by EU Measures: Insights from Germany, Greece, Latvia and Sweden*, in *Seminars in Cancer Biology*, 2022, vol. 84, p. 272.

[32] Art. 5, parr. 3 e 4, TUE.

[33] Sentenze della Corte del 4 ottobre 2024, causa C-21/23, *Lindenapotheke*, ECLI:EU:C:2024:846, punto 57; del 28 aprile 2022, causa C-319/20, *Meta Platforms I*, ECLI:EU:C:2022:322, punto 57.

[34] Conclusioni dell'Avvocato generale de La Tour del 2 dicembre 2021, causa C-319/20, *Meta Platforms I*, ECLI:EU:C:2021:979, punto 52, relativa all'interpretazione dell'art. 81, par. 2, GDPR che consente agli Stati membri di prevedere, nel proprio diritto nazionale, l'esercizio dell'azione rappresentativa senza mandato (possibilità che non è stata sfruttata, ad esempio, dal legislatore tedesco).

[35] *Ibid.* punti 52 e 55. In dottrina, O. POLLICINO, *op. cit*., 2023, p. 583; G. DE GREGORIO, *Democratising Online Content Moderation: A Constitutional Framework*, in *Comput. Law Secur. Rev.*, 2019, vol. 36, p. 1 ss.; E. MIŠĆENIĆ, A-L. HOFFMANN, *The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)*, in *ECLIC*, 2020, n. 4, pp. 50-51 e J. WAGNER, A. BENECKE, *National Legislation within the Framework of the GDPR, Limits and Opportunities of Member State Data Protection Law*, in *Eur. Data Prot. L. Rev.*, 2016, vol. 2, n. 3, pp. 353-361. In generale, si osserva una tendenza del legislatore europeo a utilizzare lo strumento del regolamento in modo atipico. A questo proposito, ad esempio, Casolari richiama la metafora utilizzata dall'Avvocato generale Ćapeta nella sentenza *Xella*, in cui il regolamento (UE) 2019/452 sullo screening degli investimenti esteri diretti nell'Unione viene descritto come "una specie di ornitorinco, una creatura strana se paragonata al tipo 'ordinario' di regolamenti previsto dall'articolo 288 TFUE" (conclusioni del 30 marzo 2023, causa C-106/22, *Xella*, ECLI:EU:C:2023:267, punto 32), assimilando l'AIA a un regolamento *sui generis*, che lascia ampio margine di discrezionalità agli Stati membri per la sua attuazione (F. CASOLARI, *A Constitutionally Oriented Reading of the EU Artificial Intelligence Act*, in *Science, Technology and Law – Mutual Impact and Current Challenges*, 2024, p. 229).

[36] Art. 6, parr. 2, lett. e) e f), e par. 3, GDPR.

individuali da garantire agli interessati [37], nonché ai trattamenti rispetto ai quali si è ritenuto di dover prevedere un regime specifico per via della loro capacità di determinare collisioni tra diritti e libertà fondamentali [38].

Tra queste ultime, la presente analisi si concentra sulle disposizioni relative al trattamento di dati sanitari per finalità di ricerca scientifica, a cui, come noto, il GDPR dedica una pluralità di norme specifiche [39], che tengono conto della peculiarità del trattamento svolto a tali fini e della sua rilevanza sociale [40]. A seconda della prospettiva interpretativa adottata, tale regime può

---

[37] Art. 23 GDPR.

[38] Artt. 85 (libertà di espressione e d'informazione), 86 (diritto d'accesso ai documenti), 89 (la libertà delle arti e delle scienze e il diritto alla salute), 91 (libertà di pensiero, di coscienza e religione). Oltre alle disposizioni già menzionate, un elenco completo delle clausole di apertura è riportato nel documento di lavoro del personale della Commissione che accompagna la Comunicazione al Parlamento europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, SWD(2020) 115 final, del 24 giugno 2020, p. 53.

[39] Innanzitutto, l'art. 89 GDPR stabilisce che il trattamento a fini di ricerca scientifica deve essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato; poi l'art. 5, par. 1, lett. b), GDPR contiene una presunzione di non incompatibilità per i trattamenti ulteriori svolti per finalità di ricerca scientifica; l'art. 5, par. 1, lett. e), GDPR prevede una deroga al principio di limitazione della conservazione, purché vengano rispettate adeguate misure tecniche e organizzative; l'art. 9, par. 2, lett. j), GDPR deroga al divieto di trattare dati sensibili se il trattamento è finalizzato alla ricerca scientifica, proporzionato a tale finalità, rispetta l'essenza del diritto alla protezione dei dati personali e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; l'art. 14, par. 5, lett. b), GDPR consente il rilascio dell'informativa in forma non individuale, quando il titolare, per fini di ricerca scientifica, raccoglie dati personali presso terzi; gli artt. 17, par. 3, lett. d) e 21, par. 6, GDPR prevedono un regime *ad hoc* per l'esercizio, rispettivamente, del diritto di cancellazione e del diritto di opposizione in caso di trattamento di dati per finalità di ricerca. Per una compiuta analisi delle norme del GDPR relative al trattamento dei dati relativi alla salute, cfr. G. SCHNEIDER, *Health Data Pools Under European Data Protection and Competition Law. Health as a Digital Business*, Springer, Berlin, 2022, pp. 179-220.

[40] N. PURTOVA, *Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons*, in R. LEENES, N. PURTOVA, S. ADAMS (eds.), *Under Observation: The Interplay Between E-Health and Surveillance*, Springer, Berlin, 2017, p. 178, in cui la ricerca viene descritta come funzionale alla formulazione e attuazione di politiche basate sulla conoscenza al fine di "*improve the quality of life for a number of people and improve the efficiency of social services*". In senso analogo, G. BINCOLETTO, P. GUARDA, *A Proactive GDPR-Compliant Solution for Fostering Medical Scientific Research as a Secondary Use of Personal Health Data*, in *Opinio Juris in Comparatione*, 2021, vol. 1, p. 44, i quali affermano che "*[s]cientific research is indispensable for the progress of the healthcare sector. Medical research responds both to the need to achieve a high level of health protection and provision of care and to the opportunity to foster innovation and grow knowledge*". Si veda anche EU Scientific Panel for Health, *Better Research for Better Health. A Vision For Health and Biomedical Research from the Scientific Panel for Health*, 2016 e Piano Nazionale Ricerca Sanitaria 2017-2019 e 2020-2022 del Ministero della Salute italiano.

risultare estremamente favorevole [41] oppure, al contrario, fortemente penalizzante per lo svolgimento delle attività di ricerca [42]. Sebbene fin dalle prime bozze del GDPR il dibattito dottrinale abbia evidenziato opinioni divergenti sul punto [43], si osserva una tendenziale convergenza nel riconoscere che, in definitiva, gli effetti positivi o negativi delle norme concernenti i trattamenti di dati sanitari per finalità di ricerca scientifica dipendono dal modo in cui gli Stati membri hanno deciso di colmare i vuoti lasciati dal legislatore europeo [44]. In particolare, con riferimento alla definizione di

---

[41] R. DUCATO, *Data Protection, Scientific Research and the Role of Information*, in *Comput. Law Secur. Rev.*, 2020, vol. 37, p. 4 ss. L'A. individua la ragione dell'esistenza di un regime speciale nell'obiettivo di conciliare il rispetto dei diritti fondamentali degli individui, la libertà di impresa e la legittima aspettativa della società con un aumento nel livello di conoscenza. Per ulteriori riferimenti, si rinvia all'analisi svolta da G. COMANDÉ, G. SCHNEIDER, *op. cit.*, 2022(a), pp. 559-596; G. COMANDÉ, G. SCHNEIDER, *Can the GDPR Make Data Flow for Research Easier? Yes it Can, By Differentiating*, in *Comput. Law Secur. Rev.*, 2021, vol. 41, pp. 1-5; G. SCHNEIDER, *Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence*, in *JIPITEC*, 2020, vol. 11, p. 61.

[42] A. BERNIER et al., *Reconciling the Biomedical Data Commons and the GDPR: Three Lessons From the EUCAN ELSI Collaboratory*, in *Eur. J. Hum. Genet*., 2023, vol. 32, n. 1, p. 1; D. PELOQUIN et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, in *Eur. J. Hum. Genet*., 2020, vol. 28, p. 704; B. WOUTERS et al., *Putting the GDPR into Practice: Difficulties and Uncertainties Experienced in the Conduct of Big Data Health Research*, in *Eur. Data Prot. L. Rev.*, 2021, vol. 7, p. 215; R. EISS, *Confusion Over Data Privacy Law Stalls Scientific Progress*, in *Nature*, 2020, p. 498; M. SHABANI, *Will the European Health Data Space Change Data Sharing Rules? Questions of Consent and Public Interest Research Loom Large*, in *Science*, 2022, p. 1357. Preoccupazioni simili erano già state espresse con riferimento alla direttiva madre da C. VANCHIERI, *New EC Privacy Directive Worries European Epidemiologists*, in *J. Natl. Cancer Inst.*, 1993, vol. 83, p. 1022; J. STROBL, E. CAVE, T. WALLEY, *Data Protection Legislation: Interpretation and Barriers to Research*, in *BMJ*, 2000, vol. 321, p. 890; D. TOWNEND et al. (eds.), *The Data Protection Directive and Medical Research Across Europe*, Routledge, New York, 2004.

[43] Cfr. 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 *Eur. J. Health Law*, 2023, vol. 30, p. 146; S. SLOKENBERGA, *Setting the Foundations: Individual Rights, Public Interest, Scientific Research and Biobanking*, in S. SLOKENBERGA, O. TZORTZTATOU, J. REICHEL (eds.), *GDPR and Biobanking Individual Rights, Public Interest and Research Regulations across Europe, Law, Governance and Technology Series*, Springer, Berlin, 2021, p. 27; J. STARKBAUM, U. FELT, *Negotiating the Reuse of Health-data: Research, Big Data, and the European General Data Protection Regulation*, in *Big Data & Society*, 2019, vol. 6., n. 2, pp. 5-6.

[44] Per un'ampia ricognizione delle norme del GDPR che consentono agli Stati membri di integrare il testo del regolamento, cfr. il documento dell'EDPB in risposta alla domanda di chiarimenti della Commissione europea in merito all'applicazione coerente del GDPR, con un'attenzione particolare alla ricerca in campo sanitario, 2021, p. 5 ss. Sulla discrezionalità lasciata agli Stati membri in riferimento ai trattamenti per scopi di ricerca scientifica, cfr. P. QUINN, *The Anonymisation of Research Data. A Pyric Victory for Privacy that Should not be*

"ricerca scientifica" [45], al contenuto delle "garanzie adeguate" previste dall'art. 89 GDPR nonché al rapporto tra queste e le "misure appropriate" di cui all'art. 9, par. 2, lett. j), GDPR e le "ulteriori condizioni, incluse limitazioni" che gli Stati membri possono imporre *ex* art. 9, par. 4, GDPR [46].

A questo proposito, nel prosieguo, metteremo in luce come le disposizioni italiane e francesi in materia di protezione dei dati personali testimonino in modo esemplare la diversità di approcci possibili nell'attuare le norme del GDPR sul trattamento dei dati sanitari per scopi di ricerca scientifica (sezioni 2.1.1 e 2.1.2) [47]. Attraverso l'analisi comparativa dei sistemi normativi scelti, verranno evidenziati gli aspetti su cui tali discipline divergono maggiormente e le ripercussioni che interpretazioni nazionali molto differenti tra loro possono produrre sulla libera circolazione dei dati personali (sezione 2.1.3).

2.1.1. Il Codice della privacy italiano e alcuni cenni (preliminari) al Fascicolo Sanitario Elettronico

In Italia, le modalità di trattamento dei dati sanitari per finalità di ricerca variano a seconda che il trattamento sia effettuato per scopi di ricerca medica, biomedica ed epidemiologica oppure sia un trattamento di dati da parte di terzi per fini di ricerca scientifica. Nel primo caso, l'art. 110, d.lgs. n. 196/2003 (Codice della privacy) [48], come da ultimo modificato dal d.lgs. n. 101/2018,

---

Pushed too Hard by the EU Data Protection Framework?, in *Eur. J. Health Law*, 2016, vol. 24, p. 1; K. PORMEISTER, *Genetic Data and the Research Exemption: Is the GDPR Going too Far?*, in *IDPL*, 2017, vol. 7, p. 138.

[45] L'unica precisazione sul significato da attribuire a tale espressione si trova nel considerando 159 GDPR, in cui si afferma espressamente che la nozione di ricerca deve essere interpretata in senso ampio, includendo ad esempio "sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati" e altresì "gli studi svolti nell'interesse pubblico nel settore della sanità pubblica". Nonostante l'ampiezza della definizione offerta, che sembrerebbe consentire l'inclusione anche di attività di tipo commerciale, l'EDPB ha sottolineato come il significato di ricerca non deve essere "*stretched beyond its common understanding*" (linee guida del 2018, p. 27), richiamando così la necessità di preservare un nucleo semantico coerente con la sua accezione tradizionale. Sul punto, in dottrina, si rinvia a S. SLOKENBERGA, *Scientific Research Regime 2.0?, How the Proposed EHDS Regulation May Change the GDPR Research Regime*, in *TechReg,* 2022, p. 139; G. COMANDÉ, G. SCHNEIDER, *It's Time. Leveraging the GDPR To Shift the Balance Towards Research-Friendly EU Data Spaces*, in *CMLRev*., 2022(b), vol. 59, pp. 754-755; R. DUCATO, *op. cit*., 2020, p. 3.

[46] C. STAUNTON et al., *Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research*, in *Frontiers in Genetics*, 2022, vol. 13, pp. 1-10.

[47] A livello metodologico, la motivazione della scelta di concentrarsi sulla normativa italiana e francese è fornita nella sezione 2 dell'introduzione al presente lavoro.

[48] D.lgs. 30 giugno 2003, n. 196 recante il Codice in materia di protezione dei dati personali,

individua il consenso come regola generale per i trattamenti di dati relativi alla salute nell'ambito delle suddette attività di ricerca [49]. In via del tutto eccezionale, è ammessa una deroga all'obbligo di ottenere il consenso degli interessati in due ipotesi.

La prima si verifica quando il trattamento è effettuato sulla base di disposizioni di legge o di regolamento o del diritto dell'Unione in conformità all'art. 9, par. 2, lett. j), GDPR [50], incluso il caso in cui una ricerca sia finanziata dal Ministero della Salute [51]. In tali circostanze, prima dell'avvio della ricerca, il titolare è tenuto a condurre e rendere pubblica una valutazione d'impatto sulla protezione dei dati personali ai sensi degli artt. 35 e 36 GDPR (DPIA). In essa devono essere riportate le garanzie adottate ai sensi dell'art. 89, par. 1, GDPR, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato di cui all'art. 9, par. 2, lett. j), GDPR [52].

---

integrato con le modifiche introdotte dal d.lgs. 10 agosto 2018, n. 101, recente le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). A completamento di tale disciplina, vi sono le prescrizioni del Garante, tra cui le prescrizioni relative al trattamento dei dati genetici e dei dati personali per scopi di ricerca scientifica, rispettivamente allegati n. 4 e 5 al provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 (doc. web n. 9124510), del 5 giugno 2019, nonché le regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, d.lgs. 10 agosto 2018, n. 101 (provvedimento n. 515 del 19 dicembre 2018).

[49] Per un'analisi critica ed esaustiva della disposizione in oggetto, si rinvia a P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Edizioni Scientifiche Italiane, Napoli, 2023, pp. 201-223.

[50] A questo proposito, nel Provvedimento del 28 settembre 2023 (doc. web n. 9948285), il Garante sembra suggerire che il regolamento (UE) 2013/1291 – oggi abrogato dal regolamento (UE) n. 695/2021 – potrebbe costituire una base giuridica per gli studi in cui la raccolta retrospettiva di dati senza consenso avvenga nell'ambito del programma Horizon da parte di enti che siano partner del progetto (per un commento a questo provvedimento, cfr. G. FINOCCHIARO, L. GRECO, *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, in *Diritto mercato tecnologia*, 2024, p. 10).

[51] L'art. 110 Codice della privacy fa riferimento in modo specifico all'art. 12-*bis*, d.lgs. 30 dicembre 1992, n. 502, che regola i finanziamenti per la ricerca corrente e finalizzata, e stabilisce che i progetti che rientrano in tali ambiti possono trovare fondamento in questa disposizione di legge. Inoltre, il par. 6 dell'art. 12-*bis* ammette esplicitamente la possibilità che "le università, il Consiglio nazionale delle ricerche e gli altri enti di ricerca pubblici e privati, nonché imprese pubbliche e private" possano contribuire alla realizzazione di tali progetti mediante specifici accordi, contratti o convenzioni.

[52] Tali misure sono individuate nelle prescrizioni del Garante italiano sui dati genetici e sulla ricerca scientifica, oltre che nelle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica.

La seconda ipotesi di esenzione, invece, concerne le attività di trattamento per cui risulti impossibile acquisire il consenso degli interessati, o ciò comporti uno sforzo sproporzionato, ovvero rischi di compromettere in modo significativo o rendere impossibile il conseguimento delle finalità della ricerca, per ragioni di natura etica, organizzativa o sanitaria [53]. Anche in questi casi, è richiesta l'adozione di misure appropriate per la tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato, insieme alla redazione di un programma di ricerca oggetto di motivato parere favorevole del comitato etico competente a livello territoriale e la redazione di una DPIA soggetta alla consultazione preventiva dell'autorità di controllo nazionale (Garante) *ex* art. 36 GDPR [54].

Durante la pandemia da Covid-19, sono state introdotte alcune deroghe temporanee al rispetto dell'art. 110 Codice della privacy. In particolare, è stata sospesa l'obbligatoria sottoposizione preventiva del progetto di ricerca e della relativa DPIA alla consultazione del Garante per specifiche categorie di soggetti, tra cui gli operatori del Servizio nazionale di protezione civile e del Servizio Sanitario Nazionale (SSN), al fine di migliorare la gestione dell'emergenza sanitaria [55]. Inoltre, è stata concessa all'Agenzia Italiana del Farmaco (AIFA) la possibilità di accedere a tutti i dati relativi agli studi sperimentali e agli usi compassionevoli dei medicinali, previa valutazione del Comitato Tecnico Scientifico dell'AIFA e del comitato etico competente [56].

Per quanto riguarda il trattamento ulteriore dei dati sanitari per finalità di ricerca scientifica da parte di un soggetto terzo, l'art. 110-*bis* Codice della privacy prevede la possibilità di derogare, *ex* art. 14, par. 5, lett. b), GDPR, al diritto dell'interessato a ricevere informazioni qualora risulti impossibile, comporti uno sforzo sproporzionato o rischi di compromettere in modo significativo il conseguimento delle finalità di ricerca, per motivi etici, organizzativi o di salute. Tuttavia, tale deroga richiede l'ottenimento dell'autorizzazione del Garante, anche mediante provvedimenti generali. Inoltre, in conformità all'art. 89 GDPR, è necessaria l'adozione di garanzie adeguate per tutelare i diritti, le libertà e gli interessi legittimi dell'interessato [57]. La medesima

[53] Si vedano le prescrizioni del Garante italiano sulla ricerca scientifica, punto 5.3.

[54] Come vedremo al termine di questa sottosezione, il d.l. del 2 marzo 2024, n. 19, convertito con modificazioni dalla legge 29 aprile 2024, Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza, è intervenuto sul testo dell'art. 110 Codice della privacy, eliminando il requisito della consultazione preventiva del Garante.

[55] Art. 14, d.l. 9 marzo 2020, n. 14, Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza Covid-19.

[56] Art. 17, d.l. 17 marzo 2020, n. 18, Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da Covid-19.

[57] Per un commento critico della disposizione in questione, si rinvia all'analisi di P. AURUCCI, *op. cit*., 2023, pp. 223-231.

disposizione prevede, infine, un regime di favore per gli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) [58] che, in ragione del carattere strumentale della loro attività rispetto alla ricerca, possono beneficiare della presunzione di non incompatibilità, fermo restando il rispetto delle condizioni di cui all'art. 89 GDPR [59].

Al quadro appena delineato sono state introdotte novità rilevanti per via di vincoli esterni cogenti, come quelli imposti dall'Unione nell'ambito del *Next Generation EU* [60]. Per consentire il raggiungimento degli obiettivi del Piano Nazionale di Ripresa e Resilienza (PNRR), ad esempio, è stato emanato il d.l. n. 139/2021 [61]. L'art. 9 di tale decreto ha modificato sensibilmente talune disposizioni del Codice della privacy in materia di trattamento dei dati personali da parte delle pubbliche amministrazioni. In particolare, questa disposizione, intervenendo sugli artt. 2-*ter* e 2-*sexies* Codice della privacy [62], ha ampliato "il novero delle fonti legittimanti i trattamenti svolti ai fini di interesse pubblico delegificando e così semplificando l'attività amministrativa prodromica

[58] Gli IRCCS sono enti del Servizio Sanitario Nazionale di rilevanza nazionale, dotati di autonomia e personalità giuridica, che operano secondo standard di eccellenza perseguendo finalità di ricerca – prevalentemente clinica e traslazionale – nel settore biomedico, nonché nell'organizzazione e gestione dei servizi sanitari. A ciò affiancano l'erogazione di prestazioni di ricovero e cura ad alta specializzazione (art. 1, d.lgs. 16 ottobre 2003, n. 288, Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico, a norma dell'art. 42, comma 1, legge 16 gennaio 2003, n. 3).

[59] Secondo l'art. 110-*bis*, par. 4, Codice della privacy, il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli IRCCS non costituisce trattamento ulteriore. In questi casi, dunque, gli IRCCS possono limitarsi a rispettare le garanzie di cui all'art. 89 GDPR, senza però dover dimostrare l'esistenza di un fondamento giuridico lecito. Sul punto, cfr. FAQ del Garante privacy sui presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca, 2024.

[60] Regolamento (UE) 2020/2094 del Consiglio del 14 dicembre 2020 che istituisce uno strumento dell'Unione europea per la ripresa, a sostegno della ripresa dell'economia dopo la crisi COVID-19. Sul NGEU, si rivia, *inter alia*, a P. DERMINE, *Le plan de relance "Next Generation EU" de l'Union européenne – Analyse constitutionnelle d'une initiative historique*, Bruylant, Bruxelles, 2023; M. LEINO, P. RUFFERT, *Next Generation EU and its Constitutional Ramifications – A Critical Assessment*, in *CMLRev*., 2022, vol. 59, pp. 433-472; B. DE WITTE, *The European Union's COVID-19 Recovery Plan: The Legal Engineering of an Economic Policy Shift*, in *CML Rev*., 2021, vol. 58, pp. 635-682.

[61] D.l. dell'8 ottobre 2021, n. 139, Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, convertito con modificazioni dalla legge n. 205/2021.

[62] Se l'art. 2-*ter* Codice della privacy riguarda i trattamenti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, l'art. 2-*sexies* Codice della privacy concerne i trattamenti di categorie particolari di dati per motivi di interesse pubblico rilevante.

all'avvio di un trattamento" [63]. Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico può ora essere giustificato non solo dalla legge e, nei casi previsti da questa, dal regolamento, ma anche da un atto amministrativo generale che ne definisce le finalità [64].

Si osservi, inoltre, il tentativo del legislatore italiano di ridimensionare i poteri conferiti al Garante [65] tramite l'abrogazione dell'art. 2-*quindecies* Codice della privacy, ossia dell'automatismo che prevedeva l'obbligatoria sottoposizione alla consultazione preventiva delle DPIA riguardanti trattamenti di dati personali svolti per l'esecuzione di un compito di interesse pubblico [66], e la limitazione delle ipotesi in cui il Garante è tenuto a presentare un parere al legislatore in vista dell'adozione di una disciplina relativa al trattamento dei dati [67]. Questo ridimensionamento è in parte condivisibile, specialmente alla luce delle posizioni di forte tutela delle prerogative individuali rispetto a quelle della collettività, con riferimento ad esempio ai trattamenti di dati sanitari per la realizzazione di metodologie predittive [68]

---

[63] Audizione del Presidente del Garante per la protezione dei dati personali Prof. Pasquale Stanzione AS 2409.

[64] Per un commento alla modifica dell'art. 2-*ter* Codice della privacy che amplia il perimetro dei presupposti di liceità, v. L. CALIFANO et al., *La protezione dei dati personali, natura, garanzie e bilanciamento di un diritto fondamentale*, Giappichelli, Torino, 2023, pp. 202-203.

[65] Audizione del novembre 2021 del Prof. Marco Bassanini presso la 1° commissione permanente – affari costituzionali del Senato della Repubblica in merito al d.d.l. n. 2409 (conversione in legge del d.l. n. 139/2021, recante disposizioni in materia di accesso ad attività culturali, sportive e ricreative, organizzazione pubbliche amministrazioni e protezione dati personali). Sul punto, si noti che la scelta di porre delle limitazioni al ruolo del Garante si inserisce in un contesto normativo in cui il legislatore italiano, sfruttando il margine di discrezionalità lasciato dal GDPR (v., in particolare, l'art. 58, par. 6), ha attribuito a tale autorità una molteplicità di poteri. Tra questi, vi è il potere di adottare, ogni due anni, un provvedimento che stabilisce le misure di garanzia per rendere sicuro, *ex* art. 9, par. 4, GDPR, il trattamento dei dati genetici, biometrici e relativi alla salute (art. 2-*septies* Codice della privacy). Inoltre, il Garante può emanare regole deontologiche (art. 2-*quater* Codice della privacy), linee guida (art. 154-*bis* Codice della privacy) e dispone di poteri autorizzatori (art. 110-*bis* Codice della privacy), sostitutivi (art. 2-*septiesdecies* Codice della privacy) e sanzionatori (art. 166 Codice della privacy).

[66] Conformemente all'art. 36, par. 5, GDPR, tale obbligo permane solo qualora, a seguito della DPIA, il rischio per i diritti e le libertà delle persone fisiche rimane elevato.

[67] Art. 154, par. 5-*bis*, Codice della privacy. Similmente, si noti come anche in materia di FSE, l'art. 21, par. 1, lett. h), n. 4, d.l. del 27 gennaio 2022, n. 4, Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico, ha espunto il riferimento all'art. 154, par. 4, d.lgs. n. 196/2003, secondo il quale il Garante è chiamato a collaborare con altre autorità amministrative indipendenti nella conduzione delle rispettive funzioni.

[68] Il Garante ha adottato otto provvedimenti di ammonimento contro Regioni italiane che, su richiesta del Ministero della Salute, hanno elaborato e successivamente aggregato dati

o per finalità di medicina di iniziativa (v. *infra*) [69].

Sulla stessa linea si colloca la modifica dell'art. 110 Codice della privacy introdotta dall'art. 44, par. 1-*bis*, d.l. del 2 marzo 2024, n. 19 "Ulteriori disposizioni urgenti per l'attuazione del PNRR" [70]. Secondo la nuova formulazione, i dati personali possono essere trattati per fini di ricerca scientifica in ambito medico, biomedico ed epidemiologico anche senza il consenso dell'interessato, a condizione che: i) si ottenga il parere favorevole del comitato etico competente; ii) si rispettino le garanzie stabilite dal Garante. In questo modo, quindi, viene espunto dall'art. 110 Codice della privacy il requisito della consultazione preventiva al Garante, sostituendolo con il mero obbligo di conformarsi alle "garanzie" individuate dallo stesso ai sensi dell'art. 106, par. 2, lett. d), Codice della privacy [71]. Questa modifica è stata fortemente voluta per

sanitari dell'intera popolazione assistita regionale in assenza di un idoneo presupposto giuridico. Secondo il Garante, sebbene sia stato il Ministero a richiedere tali trattamenti e a definirne le modalità, contando sul potere conferitogli dall'art. 2-*sexies*, par. 2, lett. v), Codice della privacy, spettava alle Regioni il ruolo di titolari dei dati. Era quindi compito loro individuare una base giuridica, la quale non poteva rinvenirsi nell'art. 7, d.l. 19 maggio 2020, n. 34, convertito con modificazioni in legge 17 luglio 2020, n. 77, Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da Covid-19 ("decreto rilancio"). Tale disposizione consente infatti al Ministero della Salute, non alle Regioni, di trattare dati per lo sviluppo di metodologie predittive sull'evoluzione del fabbisogno di salute della popolazione. Cfr. provvedimenti del 24 febbraio 2022, nn. 63, 64, 65, 66, 67, 68, 69 e 70 (doc. web nn. 9752177, 9752221, 9752260, 9752299, 9752410, 752433, 9752490 e 9752524).

[69] Il Garante ha adottato tre provvedimenti sanzionatori contro aziende sanitarie che, su richiesta della Regione, avevano trattato dati sanitari a loro disposizione per condurre attività di stratificazione del rischio, volte a classificare gli assistiti in relazione al rischio di complicanze in caso di infezione da Covid-19 per individuare i percorsi diagnostici più idonei, contestando, tra le altre cose, l'assenza di una valida base giuridica. Cfr. provvedimenti del 15 dicembre 2022, nn. 414, 415 e 416 (doc. web nn. 9844989, 9845156, 9845312). Inoltre, nel 2020, il Garante ha espresso forti perplessità in riferimento al disegno di legge provinciale riguardante ulteriori misure di sostegno per le famiglie, i lavoratori e i settori economici connesse all'emergenza epidemiologica da Covid-19 e conseguente variazione al bilancio di previsione della Provincia autonoma di Trento, specialmente in merito alla base giuridica dei trattamenti effettuati nell'ambito della medicina di iniziativa (pareri dell'8 maggio 2020, n. 84, doc. web n. 9344635 e 1° ottobre 2020, n. 275, doc. web n. 9469372). Simili considerazioni sono state svolte anche in riferimento allo schema di regolamento relativo alle disposizioni attuative della legge provinciale per la medicina di iniziativa nel servizio sanitario provinciale trentino (parere del 16 dicembre 2021, n. 175, doc. web n. 9738538).

[70] Tale decreto introduce anche una modifica dell'art. 2-*sexies* Codice della privacy che consente, una volta attuata tramite successivi pareri e decreti attuativi, la condivisione di dati relativi alla salute, pseudonimizzati, tra diversi attori (ad es. Ministero della Salute, AIFA e Agenas) per finalità istituzionali.

[71] Attualmente, i documenti normativi vincolanti vigenti che potrebbero costituire le "garanzie da osservare" sono le prescrizioni relative al trattamento dei dati genetici e dei dati personali effettuato per scopi di ricerca scientifica e le regole deontologiche sulla ricerca scientifica.

facilitare lo svolgimento degli studi retrospettivi, in cui ottenere il consenso risulta spesso impossibile e la consultazione preventiva rappresenta un adempimento eccessivamente oneroso.

Oltre alle disposizioni del Codice della privacy, è importante menzionare anche quelle del d.l. n. 179/2012 sul trattamento dei dati sanitari effettuati tramite il Fascicolo Sanitario Elettronico (FSE) [72], definito come insieme di dati e documenti di tipo socio-sanitario generati da eventi clinici presenti e trascorsi riguardanti l'assistito [73], che consente il perseguimento di tre finalità principali, ossia quelle di cura (diagnosi, cura e riabilitazione), di ricerca (studio e ricerca scientifica in campo medico, biomedico ed epidemiologico) e di governo (programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza) [74].

Sebbene per alimentare il FSE non sia più richiesto il consenso dell'assistito [75], tale requisito, unitamente al rispetto del segreto professionale, rimane

---

[72] Il quadro normativo si compone del d.l. 18 ottobre 2012, n. 179, Ulteriori misure urgenti per la crescita del Paese, convertito con modificazione dalla legge 17 dicembre 2012, n. 221, e del d.p.c.m. 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico. Si vedano anche le linee guida del Garante in tema di FSE e di dossier sanitario (16 luglio 2009, doc. web n. 1634116) e le prescrizioni dello stesso in tema di FSE (16 luglio 2009, doc. web n. 1633793). Per completezza espositiva, vale la pena ricordare che, accanto alle disposizioni sul FSE, si aggiungono quelle relative all'istituzione della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza per finalità quali la promozione della ricerca scientifica in ambito oncologico (art. 1, legge 22 marzo 2019, n. 29, Istituzione e disciplina della Rete nazionale dei registri e dei tumori e dei sistemi di sorveglianza e del referto epidemiologico per il controllo sanitario della popolazione). Sul funzionamento dei sistemi di sorveglianza e dei registri di mortalità, tumori e altre patologie, si rinvia altresì all'art. 12, parr. 10-14, d.l. n. 179/2012.

[73] Art. 12, par. 1, d.l. n. 179/2012. Con l'art. 21, par. 1, lett. a-*bis*), d.l. 27 gennaio 2022, n. 4, convertito con modificazioni dalla legge 28 marzo 2022, n. 25 ("decreto Sostegni-*ter*"), viene specificato che l'inserimento di ogni prestazione sanitaria erogata da operatori pubblici, privati accreditati e privati autorizzati deve avvenire entro 5 giorni dalla prestazione stessa.

[74] Art. 12, par. 2, d.l. n. 179/2012. V. anche gli artt. 18-19, d.p.c.m. n. 178/2015. Per completezza espositiva, occorre sottolineare che l'art. 21, par. 1, lett. a-*bis*), d.l. 27 gennaio 2022, n. 4 ha attribuito un rilievo autonomo alla prevenzione (oggi inserito in una specifica lett. a-*bis*, dell'art. 12, par. 2) e ha aggiunto il riferimento alla "profilassi internazionale" (lett. a-*ter* del medesimo articolo).

[75] Modifica derivante dall'abrogazione dell'art. 12, par. 3-*bis*, d.l. n. 179/2012 da parte dell'art. 11, d.l. 19 maggio 2020, n. 34 (sulla lettura distorsiva di tale norma che è stata data nella prassi, cfr. R. Miccù, *Questioni attuali introno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in *federalismi.it*, 2021, vol. 5, pp. 12-13). Il "decreto rilancio" ha inoltre ampliato il novero di dati che confluiscono nel FSE (oltre a quelli relativi alle prestazioni erogate nell'ambito del SSN, anche quelli concernenti a professionisti che operano privatamente all'esterno del SSN per finalità di cura) e ha permesso l'alimentazione del FSE attraverso l'Infrastruttura Nazionale di Interoperabilità, integrando i dati relativi al consenso, alla donazione di organi e tessuti, quelli riguardanti la situazione vaccinale contenuti nelle anagrafi vaccinali regionali e quelli relativi al Centro unico di prenotazione di ciascun sistema regionale.

per la consultazione dei dati presenti nel FSE per le finalità di cura, prevenzione e profilassi internazionale [76], salvo i casi di emergenza sanitaria [77], o in presenza di impossibilità fisica, incapacità di agire, o incapacità di intendere e volere dell'interessato, nonché in situazioni di grave, imminente e irreparabile rischio per la salute e l'incolumità fisica dell'interessato [78]. Con riferimento, invece, alle finalità di ricerca e programmazione sanitaria, le regioni, le province autonome, il Ministero del lavoro e delle politiche sociali, il Ministero della Salute e l'Agenzia nazionale per i servizi sanitari regionali (Agenas) possono trattare i dati (privi di identificativi) presenti nel FSE sulla base delle disposizioni contenute nel decreto del Ministero della Salute [79], il quale, tuttavia, come vedremo in seguito, non contiene ancora norme specifiche in merito [80].

2.1.2. La legge francese sulla protezione dei dati e il sistema centralizzato dell'*Health Data Hub*

In Francia, il trattamento dei dati personali è disciplinato dalla *loi 78-17/78 relative à l'informatique, aux fichiers et aux libertés* (LIL), così come modificata dalla *loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles* e dal *décret n° 2019-536 du 29 mai 2019*. Per quanto riguarda l'uso dei dati sanitari per fini di ricerca scientifica, la LIL prevede regole specifiche applicabili ai trattamenti realizzati nell'interesse pubblico, ad esempio per garantire elevati standard di qualità e sicurezza nei servizi sanitari, nei prodotti farmaceutici e nei dispositivi medici [81].

Le procedure da seguire differiscono in base all'ambito e alla categoria della ricerca, dovendo distinguere tra ricerca interna e ricerca multicentrica [82]. Nel primo caso, ossia quando i dati vengono raccolti nell'ambito del monitoraggio

---

[76] Come evidenziato, le finalità di cura e prevenzione devono essere perseguite dai soggetti del SSN e dai servizi socio-sanitari regionali e da tutti gli esercenti le professioni sanitarie, nonché, per le finalità di prevenzione, dagli Uffici delle Regioni e delle Province autonome competenti in materia (art. 12, parr. 4 e 4-*bis*, d.l. n. 179/2012). Al contrario, le finalità di profilassi internazionale spettano unicamente al Ministero della Salute (art. 12, par. 4-*ter*, d.l. n. 179/2012).

[77] Art. 12, par. 5, d.l. n. 179/2012.

[78] Art. 20 del decreto del Ministero della Salute del 7 settembre 2023, Fascicolo sanitario elettronico 2.0, GU Serie Generale n. 294 del 24 ottobre 2023.

[79] Art. 12, par. 6, d.l. n. 179/2012.

[80] Si rimanda alla sezione 3.2.2 del presente capitolo.

[81] Artt. 44 e 64-77 LIL.

[82] Cfr. https://www.cnil.fr/fr/recherche-medicale-quel-est-le-cadre-legal. Un discorso a parte deve essere fatto per le ricerche in cui si utilizzano dati genetici e per cui è richiesta l'acquisizione del consenso espresso e informato dell'interessato.

del paziente per uso esclusivo del personale, non è richiesta alcuna formalità particolare, ad eccezione: i) dell'adempimento degli oneri informativi di cui agli artt. 13 e 14 GDPR; ii) delle registrazione dei trattamenti di dati nel registro delle attività di trattamento del titolare; iii) per le ricerche che coinvolgono la persona umana, del parere favorevole del *Comité compétent de protection des personnes* (CPP).

Nel secondo caso, invece, relativo alla ricerca multicentrica (o che implica l'accesso ai dati da parte di soggetti esterni all'équipe di cura) [83], si applica un regime autorizzatorio [84]. Per condurre legittimamente questo tipo di ricerca, infatti, è necessario presentare una *demande d'autorisation "recherche"*, dopo la quale la *Commission Nationale de l'Informatique et des Libertés* (CNIL) può decidere di rilasciare un'autorizzazione vincolante entro due mesi, previa consultazione del comitato etico competente: CPP o *Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé* (CESREES) [85]. Qualora il progetto di ricerca subisse modifiche sostanziali (ad es. nuova identità del titolare o nuova domanda di ricerca), benché rimanga imperativo l'obbligo di darne comunicazione agli interessati, non sempre è richiesta una nuova autorizzazione della CNIL, a condizione che si dimostri il rispetto delle *méthodologies de référence* (MR) della CNIL pertinenti [86].

Tuttavia, questo regime non si applica agli studi che utilizzano dati genetici, per i quali è necessario ottenere il consenso esplicito e informato

---

[83] Ai sensi dell'art. 1110-12 *Code de la santé publique*, con équipe di cura si intende "un insieme di professionisti che partecipano direttamente, a beneficio del paziente stesso, all'esecuzione di attività diagnostiche, terapeutiche, compensative di disabilità, analgesiche o di prevenzione della perdita di autonomia, ovvero alle azioni necessarie per il coordinamento di alcuni di questi atti, e che: i) lavorano nello stesso istituto sanitario, all'interno del servizio sanitario delle forze armate, nello stesso istituto o servizio sociale o medico-sociale di cui all'articolo I dell'articolo L. 312-1 del Codice dell'azione sociale e delle famiglie o nell'ambito di una struttura di cooperazione, esercizio condiviso o coordinamento sanitario o medico-sociale figurante in un elenco fissato con decreto; ii) o sono stati riconosciuti come membri dell'équipe assistenziale dal paziente che li contatta per l'esecuzione delle consultazioni e delle procedure prescritte da un medico a cui ha affidato le cure; iii) lavorano in gruppo, comprendente almeno un operatore sanitario, con un'organizzazione formalizzata e pratiche conformi a specifiche stabilite con ordinanza del Ministro responsabile della salute" (traduzione dell'autore).

[84] Artt. 66 e 76 LIL.

[85] All'art. 76 LIL viene specificato che, per le domande che prevedono il coinvolgimento della persona umana, la comunicazione deve essere rivolta al CPP, mentre per le altre, al CEREES.

[86] Sul sito della CNIL è possibile trovare una descrizione particolarmente dettagliata dei passaggi da seguire in queste ipotesi: https://www.cnil.fr/fr/modification-dun-traitement-de-donnees-ayant-pour-finalite-une-recherche-une-etude-ou-une-evaluation.

dell'interessato [87], né alle ricerche rigorosamente conformi alle MR [88], per le quali è sufficiente presentare una dichiarazione di conformità all'autorità di controllo [89]. Nella definizione delle MR, la CNIL adotta un approccio favorevole al trattamento dei dati per finalità di ricerca se giustificato da un interesse pubblico o un interesse legittimo. I principali adempimenti riguardano la nomina di un responsabile della protezione dei dati (DPO), l'informazione degli interessati, che può anche avvenire tramite la pubblicazione delle informazioni sul sito del titolare del trattamento, e il parere del comitato etico. Grazie alle MR, quindi, le formalità relative al trattamento dei dati per scopi di ricerca in campo sanitario vengono semplificate, bilanciando la protezione dei diritti degli interessati con la promozione della ricerca, dell'innovazione e della competitività.

Per quanto riguarda i dati raccolti nell'ambito del Sistema Nazionale dei Dati Sanitari (SNDS) è stato istituito un comitato di audit a supporto del lavoro della CNIL, con il compito di stabilire le strategie per mettere a disposizione questi dati a fini di ricerca, studio e valutazione [90]. Questi scopi sono stati ampliati a seguito delle modifiche introdotte dalla *loi 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé* che è intervenuta sul *Code de la santé publique*. Nello stesso anno, il governo francese ha creato anche la *Plateforme des données de santé* o *Health Data Hub* (HDH), termine con cui ci si riferisce sia alla piattaforma tecnologica che rappresenta il punto di accesso unico per i dati sanitari raccolti per finalità di cura nel SNDS sia al gruppo di interesse pubblico (GIP) responsabile della gestione di tale piattaforma [91].

---

[87] Art. 75 LIL.

[88] Le MR non sono altro che regole di riferimento, formalmente non vincolanti, che descrivono metodologie e pratiche che consentono al titolare di rendere la sua attività di trattamento conforme alla normativa.

[89] Art. 73 LIL. Le MR finora elaborate sono otto e ognuna di esse ha un diverso ambito di applicazione. Nello specifico, per le ricerche che coinvolgono la persona umana, si deve fare riferimento a MR-001 (ricerca in campo sanitario con acquisizione del consenso) e MR-002 (studi sulle prestazioni non interventistiche per dispositivi medico-diagnostici in vitro) o MR-003 (ricerca nel campo della salute senza ottenere il consenso), mentre per quelle che non prevedono tale coinvolgimento, si rinvia a MR-004 (ricerche che non coinvolgono esseri umani e si riferisce a studi che riutilizzano i dati di salute alla luce di un interesse pubblico), MR-005 (studi che richiedono l'accesso ai dati PMSI e/o RPU da parte di strutture sanitarie e federazioni ospedaliere) o MR-006 (studi che richiedono l'accesso ai dati PMSI da parte di produttori di prodotti sanitari). Recentemente, sono state introdotte anche le MR-007 e MR-008, di cui parleremo nella sezione 2.2.2 del presente capitolo.

[90] Art. 77 LIL.

[91] *Arrêté du 29 novembre 2019* portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public "Institut national des données de santé" portant création

Secondo la normativa francese [92], una volta verificata dal GIP la completezza della domanda e, dal comitato etico competente, le finalità dello studio e il requisito dell'interesse pubblico, spetta alla CNIL fornire, entro un mese, un parere non vincolante sulla richiesta di accesso ai dati. Successivamente, l'Autorità francese deve decidere se autorizzare o meno la domanda [93], dopo aver verificato il rispetto delle libertà individuali e la presenza di adeguate misure di sicurezza, salvo nei casi in cui si dimostri la conformità alle MR pertinenti. In seguito all'autorizzazione e alla registrazione dei progetti di ricerca nel registro pubblico di HDH, i dati vengono messi a disposizione per specifiche finalità di interesse pubblico [94], sotto forma di statistiche aggregate o in modo da rendere impossibile l'identificazione [95].

2.1.3. L'imperfetta coincidenza tra le disposizioni nazionali e i possibili effetti sulla libera circolazione dei dati

L'analisi condotta nei paragrafi precedenti mostra come, in entrambi gli ordinamenti presi in considerazione, il trattamento dei dati sanitari a fini di ricerca scientifica è disciplinato da regole specifiche, seppur in parte divergenti. Al di là della centralità del ruolo delle autorità di controllo e dei comitati etici, numerose disposizioni riflettono la mancanza di un approccio regolatorio uniforme. Si pensi, ad esempio, alle differenze relative alla base giuridica per i trattamenti di dati a fini di ricerca e alle garanzie introdotte *ex* artt. 89 e 9, parr. 2, j) e 4, GDPR. Mentre il Codice della privacy individua il consenso come fondamento normativo obbligatorio nella maggior parte dei casi per i trattamenti di dati a fini di ricerca, la normativa francese adotta un approccio differente, escludendo tale obbligo, salvo per i trattamenti che riguardano dati genetici e mirando piuttosto a semplificare le procedure di accesso ai dati.

---

du groupement d'intérêt public "Plateforme des données de santé". La composizione del gruppo di interesse appare particolarmente variegata, comprendendo, tra gli altri, rappresentanti del Ministero della Salute e della Ricerca, di ospedali universitari e dei consigli nazionali dei medici e dei farmacisti.

[92] Sezione 3, capo III del titolo II, LIL e artt. L1461-1 ss. *Code de la santé publique*.

[93] Art. 66, par. 5, LIL, in cui si specifica che, se entro il termine di due mesi, la CNIL non si esprime, la richiesta di autorizzazione si intende accolta.

[94] L'art. L1461-1, parr. 3 e 5, *Code de la santé publique* menziona, *inter alia*, le finalità di ricerca, gli studi, la valutazione e l'innovazione nei settori dell'assistenza sanitaria e medico-sociale, mentre sono vietati trattamenti per la promozione di particolari prodotti (ad es. dispositivi medici) agli operatori sanitari o alle strutture sanitarie, oppure per l'esclusione delle garanzie dai contratti assicurativi e la modifica dei contributi o dei premi assicurativi per un individuo o un gruppo di individui che presentano lo stesso rischio.

[95] Art. L1461-2 *Code de la santé publique*.

Da un lato, per le ricerche interne, i principali adempimenti da compiere si riducono all'assolvimento di meri oneri informativi. Dall'altro, per le ricerche multicentriche, l'obbligo di ottenere l'autorizzazione della CNIL, quale requisito supplementare rispetto a quelli contenuti agli artt. 9, par. 2, lett. j) e 89 GDPR, in attuazione dell'art. 9, par. 4, GDPR, può essere facilmente evitato presentando una dichiarazione di conformità alle MR presentata dal titolare del trattamento. In questa direzione vanno anche le novità del 2019 riguardanti l'accesso ai dati raccolti per finalità di cura nell'ambito del SNDS tramite HDH. Questo sistema, come vedremo, anticipa quanto previsto dallo EHDS per l'uso secondario dei dati sanitari elettronici.

In Italia, invece, anche nelle ipotesi in cui è consentito derogare all'obbligo di ottenere il consenso, gli adempimenti rimangono onerosi. Prima della modifica del d.l. n. 19/2024, infatti, il titolare era tenuto a consultare preventivamente il Garante, indipendentemente dall'esito della DPIA e, quindi, dall'eventuale presenza di rischi residui non mitigabili [96]. Ciò rifletteva una visione del legislatore italiano secondo cui il livello di rischio doveva essere considerato, di per sé, intrinsecamente elevato in quelle situazioni in cui non fosse possibile informare gli interessati, o quando tale informazione risultasse sproporzionata, o ancora potesse compromettere il raggiungimento degli obiettivi del trattamento. Al contrario, in Francia, la consultazione preventiva viene richiesta solo se, a seguito della DPIA, il titolare del trattamento riconosca di non essere in grado di mitigare opportunamente i rischi associati al trattamento in questione [97].

Con l'eliminazione dell'obbligo di consultazione preventiva dal Codice della privacy, sebbene vi sia una chiara riduzione degli oneri per coloro che intendono trattare i dati per fini di ricerca scientifica, tali soggetti sono comunque tenuti a conformarsi alle misure di garanzia [98] e alle regole deontologiche stabilite dal Garante [99], in attuazione dell'art. 9, par. 4, GDPR. A questo proposito, non è irrealistico ipotizzare che, alla luce delle prassi dell'autorità di controllo italiana (v. *infra*) [100], queste ultime vengano modificate per

[96] Art. 110 Codice della privacy.

[97] Art. 63 LIL.

[98] Art. 2-*septies* Codice della privacy

[99] Artt. 2-*quater* e 106 Codice della privacy. Nell'ordinamento italiano, una violazione delle regole deontologiche determina una violazione del principio di cui all'art. 5, par. 1, lett. a), GDPR, in quanto – diversamente dai codici di condotta – tali regole sono "collocate nel sistema delle fonti e il loro rispetto è posto a condizione essenziale di liceità e correttezza del trattamento" (R. D'ORAZIO, *Art. 2-quater*, in R. D'ORAZIO et al., *Codice della privacy e data protection*, Giuffrè, Milano, 2021, pp. 1031-1032).

[100] In particolare, sezione 2.2.1.

compensare l'alleggerimento del regime, in modo da rafforzare la tutela dei diritti degli interessati [101].

In aggiunta, benché non sia stato evidenziato nelle sottosezioni precedenti, è importante notare che tra le normative esaminate emergono ulteriori differenze riguardo alla possibilità di prevedere deroghe ai diritti degli interessati *ex* art. 89, par. 2, GDPR. Mentre il legislatore italiano ha introdotto un'unica deroga rispetto al diritto di rettifica, consentendo l'annotazione delle modifiche richieste senza intervenire sui dati [102], il legislatore francese ammette la possibilità di derogare a tutti i diritti degli interessati previsti dall'art. 89 GDPR, inclusi quindi i diritti di accesso, rettifica, limitazione e opposizione [103].

Queste disparità nell'applicazione delle norme del GDPR possono avere ripercussioni, oltre che sul livello di tutela dei diritti fondamentali degli interessati, anche sulla capacità di condurre ricerca collaborativa, soprattutto osservazionale e retrospettiva, tra Stati membri. In prospettiva più ampia, esse rischiano di compromettere la realizzazione dell'obiettivo della libera circolazione dei dati personali all'interno dell'Unione [104]. In mancanza di

---

[101] Questa direzione sembra già emergere dal provvedimento del 9 maggio 2024 del Garante per la protezione dei dati personali (doc. web n. 10016146), in cui vengono individuate le garanzie per i trattamenti di dati relativi alla salute a fini di ricerca medica, biomedica e epidemiologica. Rispetto alle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica del 2018 (par. 5.2), il Garante specifica che il titolare deve: i) adottare misure appropriate a tutelare i diritti, le libertà e gli interessi legittimi degli interessati; ii) acquisire il parere del comitato etico; iii) documentare gli sforzi profusi per tentare di contattare nuovamente gli interessati (circostanza che è da considerarsi in ogni caso "del tutto residuale"); iv) svolgere e pubblicare una DPIA.

[102] Art. 110, par. 2, Codice della privacy, da integrare con l'art. 12 delle regole deontologiche sulla ricerca scientifica, in cui si stabilisce che "[q]ualora, in caso di esercizio dei diritti di cui agli artt. 15 e s.s. del Regolamento, sono necessarie modifiche ai dati che riguardano l'interessato, il titolare del trattamento provvede ad annotare, in appositi spazi o registri, le modifiche richieste all'interessato, senza variare i dati originariamente immessi".

[103] Art. 49, par. 3, n. 2 e 78 LIL. Scelta condivisa, ad esempio, anche dal legislatore finlandese. Secondo la sezione 31, par. 1, i diritti contenuti negli artt. 15, 16, 18 e 21 possono essere derogati quando il trattamento si fonda su un progetto di ricerca adeguato, è stato designato un responsabile per la ricerca e i dati personali sono usati e messi a disposizione solo per finalità di ricerca scientifica o per altri scopi compatibili e unicamente a soggetti autorizzati. A queste garanzie si aggiunge, in caso di trattamento di dati appartenenti a categorie particolari, lo svolgimento di una DPIA, da inviare per informazione all'autorità di controllo, oppure il rispetto di codici di condotta dove si prendono in considerazione ipotesi di deroga dei diritti degli interessati.

[104] EDPS, *Study on the Appropriate Safeguards Under Article 89(1) GDPR for The Processing of Personal Data for Scientific Research*, 2019, p. 62. In senso analogo, nel *workshop* organizzato da EMA sul GDPR e sull'uso secondario nel 2020, si sottolinea come in "*[s]everal EU projects the planned data sharing has been delayed, due to legal uncertainties(for instance*

un'armonizzazione a livello europeo, i titolari coinvolti in progetti di ricerca transnazionale potrebbero infatti essere tenuti a conformarsi a requisiti diversi, alcuni dei quali più ostativi di altri rispetto all'uso e alla condivisione dei dati personali [105].

Scenari di questo tipo, che danno luogo a veri e propri "*intra-EU conflict of laws*" [106], risultano particolarmente problematici dal momento che il GDPR non contiene alcuna disposizione specifica sul diritto nazionale applicabile. Diversamente dalla DPD [107], infatti, l'unico riferimento del GDPR a tale

---

uncertainties with regards to anonymization and broad consent) as well as due to the lack of harmonisation regarding the application of GDPR by Member States". Cfr. https://www.ema.europa.eu/en/events/workshop-general-data-protection-regulation-gdpr-secondary-use-data-medicines-public-health-purposes. Esempi di questo tipo sono i progetti finanziati con il programma Horizon 2020 di finanziamento della ricerca e dell'innovazione dell'Unione. Cfr. https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-2020_it. In dottrina, gli effetti del GDPR sulla fattibilità di progetti di ricerca collaborativi sono stati evidenziati, *inter alia*, da B.A. SIMELL et al., *Transnational Access to Large Prospective Cohorts in Europe: Current Trends and Unmet Needs*, in *New Biotechnology*, 2019, vol. 49, pp. 102-103; T. RABESANDRATANA, *European Data Law is Impeding Studies on Diabetes and Alzheimer's, Researchers Warn*, in *Science*, 2019; A. WIEBE, N. DIETRICH, *Open Data Protection: Study on Legal Barriers to Open Data Sharing, Data Protection and PSI*, Universitätsverlag Göttingen, 2017, pp. 192-201. Esula, invece, dall'analisi del presente contributo l'esame delle conseguenze che la conformità alle norme del GDPR produce sui progetti collaborativi tra paesi dell'Unione e paesi extra-UE. Sul punto si rinvia a A. BERNIER et al., *op. cit.*, 2023, p. 7.

[105] G. DI FEDERICO, S. NEGRI, *Unione europea e salute. Principi, azioni, diritti e sicurezza*, Cedam, Milano, 2019, pp. 248-249: gli A. sottolineano che "[l]e deroghe ai diritti dei pazienti risultano alquanto generiche che lasciano ampio margine discrezionale agli Stati membri e sono quindi suscettibili di impattare negativamente sulla ricerca in campo sanitario condotta a livello sovranazionale, cioè quella che maggiormente dovrebbe beneficiare dell'azione di sostegno dell'Unione".

[106] K. PORMEISTER, *Genetic Research and Applicable Law: the Intra-EU Conflict of Laws as a Regulatory Challenge to Cross-border Genetic Research*, in *JLB*, 2018, vol. 5, n. 3, p. 715 ss.

[107] Art. 4, par. 1, lett. a), DPD, così come interpretato dalla giurisprudenza della Corte in *Weltimmo*. In questa occasione, è stato specificato che è possibile applicare la legge di uno Stato membro diverso da quello nel quale il titolare è registrato, a condizione che in questo Stato il titolare svolga, tramite un'organizzazione stabile, un'attività effettiva e reale, anche minima (sentenza della Corte del 1° ottobre 2015, causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639, punti 28 e 31). Inoltre, la Corte ha precisato che non è richiesto che il trattamento sia effettuato "dallo" stabilimento, ma piuttosto "nel contesto delle attività" di quest'ultimo (punto 35). Tale orientamento, confermato anche in *Amazon* (sentenza della Corte del 28 luglio 2016, causa C-191/15, *Verein für Konsumenteninformation c. Amazon EU*, ECLI:EU:C:2016:612, punti 75-78), è stato poi codificato dal GDPR, dove si afferma che "[q]ualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga

questione riguarda i trattamenti di dati per finalità giornalistiche. In questi casi, l'art. 85 GDPR stabilisce che, qualora le deroghe e le esenzioni adottate dagli Stati membri per conciliare il diritto alla protezione dei dati e la libertà di espressione "differiscano da uno Stato membro all'altro, dovrebbe applicarsi il diritto dello Stato membro cui è soggetto il titolare del trattamento" [108].

Anche ipotizzando un'estensione analogica di tale criterio ai trattamenti di dati per finalità di ricerca scientifica, permane l'incertezza su cosa debba intendersi con il "diritto dello Stato membro cui è soggetto il titolare del trattamento". In concreto, se un titolare del trattamento stabilito in uno Stato A utilizza dati raccolti da uno dei partner del consorzio con sede in uno Stato B, quale diritto nazionale trova applicazione? Quello dello Stato in cui avviene il trattamento (Stato A), quello dello Stato in cui sono raccolti i dati (Stato B), oppure entrambi [109]?

In prima battuta, potrebbe apparire naturale interrogarsi sul possibile ruolo del diritto internazionale privato dell'Unione ai fini della risoluzione delle

---

all'interno dell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica" (considerando 22 GDPR). Per una ricostruzione sull'ambito di applicazione territoriale della DPD, cfr. M. BRKAN, *Data Protection and Conflict-of-Laws: A Challenging Relationship*, in *Eur. Data Prot. L. Rev*., 2016, vol. 2, pp. 324-341, mentre del GDPR, cfr., *inter alia*, K. PORMEISTER, *op. cit*., 2018, pp. 706-723.

[108] Considerando 153 GDPR.

[109] Particolarmente interessanti sul punto sono le considerazioni effettuate da Pormeister che si domanda quanto segue: "*If a research entity in a given Member State wants to incorporate genetic data from people across Europe into their dataset, the following questions are likely to arise. If the data have been obtained for research based on consent, the law of which Member State applies to that consent, and how broad can the consent under the applicable national law be? Does the consent have to comply with the rules of the Member State in which it was obtained, or with those of the Member State in which research is to be conducted (or both)? If these rules differ, which ones should be applied? If the data have been obtained for other purposes (eg healthcare) or the consent does not cover the planned research activities, in order to use the data in research without having to obtain (new) consent, should the researcher follow the rules of the country in which he operates, or those of the Member States in which the data have been obtained from the individuals? Regardless of the legal basis for the use of the data, which individuals could possibly invoke the right to object under Article 21 GDPR? Although Article 21(6) GDPR provides for a directly applicable exception in the research context, this is limited to cases where the processing is necessary for the performance of a task carried out for reasons of public interest. Otherwise, the applicability of the right to object will depend on Member State law (See Arts. 9(2)(j) and 89(2) GDPR). If the law applicable to the research would be the one of the Member State where the research entity carries out its activities, the research entity could rely on that single set of rules. However, if applicable law would depend on where the data were obtained from individuals (ie most likely the Member State of residence of the individual), the research entity would essentially have to apply different rules to one dataset*" (K. PORMEISTER, *op. cit*., 2018, p. 714).

questioni transfrontaliere connesse all'applicazione del GDPR. Tuttavia, un riferimento diretto ai regolamenti Roma I [110] e Roma II [111] richiederebbe preliminarmente di affrontare la questione, tutt'altro che agevole, della qualificazione del rapporto giuridico rilevante ai fini internazional-privatistici. La giurisprudenza tende a escludere la natura contrattuale del rapporto in assenza di un'obbligazione liberamente assunta da una parte nei confronti dell'altra [112], circostanza che ricorre solo eccezionalmente nelle ipotesi di trattamento illecito dei dati personali. Una qualificazione alternativa in termini di obbligazione extracontrattuale non conduce, peraltro, a risultati più soddisfacenti: il regolamento Roma II, pur disciplinando in via generale le obbligazioni extracontrattuali, esclude infatti dal proprio ambito di applicazione quelle derivanti da violazioni della vita privata e dei diritti della personalità [113], categoria nella quale sembrano potersi ricondurre, almeno in parte, le lesioni del diritto fondamentale alla protezione dei dati personali.

Alla luce di tali incertezze, un ricorso diretto ai regolamenti Roma I o Roma II rischierebbe di fondarsi su presupposti metodologicamente fragili e di condurre a soluzioni poco coerenti con la logica sottesa al GDPR. Quest'ultimo, in quanto normativa *ad hoc* per la protezione dei dati personali e ad applicazione tendenzialmente uniforme, è concepito per garantire un elevato livello di tutela degli interessati e per evitare che il ricorso a criteri di collegamento eterogenei o a scelte opportunistiche della legge applicabile comprometta la libera circolazione dei dati personali nell'Unione. Cionondimeno, l'assenza nel GDPR di criteri espliciti per la determinazione del diritto nazionale applicabile nei casi transfrontalieri lascia aperti margini di incertezza che, in concreto, possono favorire fenomeni di *forum shopping*, incidendo negativamente tanto sulla certezza del diritto quanto sull'effettività delle garanzie riconosciute agli interessati e sui costi di conformità gravanti sui titolari del trattamento [114].

---

[110] Regolamento (CE) 593/2008 del Parlamento europeo e del Consiglio, del 17 giugno 2008, sulla legge applicabile alle obbligazioni contrattuali (Roma I).

[111] Regolamento (CE) 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II).

[112] Sentenze della Corte del 17 giugno 1992, causa C-26/91, *Handte*, ECLI:EU:C:1992:268, punto 15; del 27 ottobre 1998, causa C-51/97, *Réunion européenne*, ECLI:EU:C:1998:509, punto 17; del 17 settembre 2002, causa C-334/00, *Tacconi*, ECLI:EU:C:2002:499, punto 23; del 20 gennaio 2005, causa C-27/02, *Engler*, ECLI:EU:C:2005:33, punti 51-53; del 28 gennaio 2015, causa C-375/13, *Kolassa*, ECLI:EU:C:2015:37, punto 39.

[113] Art. 1, par. 2, lett. g), regolamento Roma II.

[114] S. SLOKENBERGA, *op. cit.*, 2021, p. 26 prende in considerazione questo tipo di problemi rispetto al rischio che il requisito di chiedere l'approvazione al comitato etico possa rappresentare un ostacolo alla libera circolazione dei dati. Sul punto, si veda anche K. PORMEISTER, *op. cit*., 2017, pp. 137-146.

2.2. La disomogeneità delle prassi amministrative

Il quadro delineato nella sezione precedente si complica ulteriormente se si considera l'elevato grado di disomogeneità nelle prassi interpretative e applicative del GDPR da parte delle autorità di controllo nazionali [115], alle quali spetterebbe il compito centrale di assicurare la coerente applicazione della normativa in questione [116]. Al contrario, come rilevato dalla Commissione nella seconda valutazione sull'applicazione del GDPR, le "autorità di protezione dei dati continuano […] ad adottare interpretazioni divergenti di vari concetti chiave in materia di protezione dei dati" [117]. Questo conferma quanto già emerso nella prima valutazione del GDPR del 2020, in cui la Commissione sottolineava che "lo sviluppo di una cultura europea veramente comune in materia di protezione dei dati tra le autorità di protezione dei dati è un processo ancora in corso" [118].

Sebbene la dimensione fattuale in cui si incardina l'attività degli interpreti precluda – o comunque limiti fortemente – le possibilità di giungere ad approcci totalmente sovrapponibili, è senz'altro auspicabile una maggiore coerenza tra gli stessi in modo da evitare che la libera circolazione dei dati ne risulti compromessa. In quest'ottica, diventa cruciale approfondire lo studio delle prassi delle autorità nazionali, per evidenziare le problematiche che potrebbero sorgere a causa di tali divergenze.

A tal fine, nel prosieguo, illustreremo alcuni esempi di prassi amministrative che appaiono indicative di disallineamenti negli approcci applicativi, con particolare attenzione alle attività di *enforcement* relative al trattamento dei dati sanitari per finalità di ricerca scientifica in ambito sanitario. L'analisi manterrà come casi studio i sistemi italiano e francese, che attribuiscono un ruolo centrale (istruttorio e autorizzatorio) all'autorità di controllo. Tuttavia, va notato che una simile comparazione non è un'operazione priva di insidie,

---

[115] Dall'ultimo report sull'applicazione del GDPR emerge chiaramente infatti che la situazione di frammentazione nell'applicazione del GDPR non deriva soltanto dall'adozione di norme di specificazione facoltative da parte degli Stati membri, quanto piuttosto dalle "interpretazioni divergenti del GDPR da parte delle autorità di protezione dei dati" (COM(2024) 357 final, p. 12).

[116] Art. 51, par. 2, e considerando 123 GDPR. L'importanza del ruolo riservato alle autorità di controllo si evince dalla scelta di menzionare tali autorità negli artt. 8, par. 3, Carta e 16, par. 2, TFUE, in cui si afferma che il rispetto delle norme relative alla protezione e libera circolazione dei dati personali "è soggetto al controllo di autorità indipendenti".

[117] COM(2024) 357 final, p. 11.

[118] COM(2020) 264 final, p. 6. Similmente, il Parlamento europeo nella sua Risoluzione del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del GDPR ha sottolineato che l'attuazione del GDPR da parte delle autorità di controllo nazionali è "disomogenea e talvolta inesistente" (P9_TA(2021)0111, p. 5).

in quanto si scontra con la presenza di informazioni limitate o messe a disposizione secondo modalità e formati non sempre coincidenti [119]. Pertanto, anziché effettuare una ricognizione empirica del numero di provvedimenti adottati o sanzioni riscosse, riteniamo più utile soffermarsi sull'iter argomentativo seguito dalle autorità di controllo nei provvedimenti da esse adottati.

2.2.1. Il Garante per la protezione dei dati personali e la tutela della persona

La denominazione stessa di "Garante per la protezione dei dati personali" appare già di per sé sintomatica dell'"approccio (particolarmente) stringente" [120] adottato dall'autorità di controllo italiana, che pone al centro della propria attività la persona e le sue prerogative, piuttosto che l'interesse a trattare i dati personali altrui. Questo orientamento è evidenziato in modo particolare dalla centralità riservata al consenso e al rispetto degli oneri informativi che emerge chiaramente dai pareri del Garante nell'ambito della procedura di consultazione preventiva *ex* art. 110, par. 1, Codice della privacy o in risposta a segnalazioni.

Nel caso relativo allo studio osservazionale e retrospettivo "*European Register for Myeloproliferative Neoplasm*" aggiornato (ERNEST 2.0) dalla Fondazione per la Ricerca Ospedale di Bergamo (FROM), il Garante ha ritenuto il trattamento illecito per violazione del principio di trasparenza e degli obblighi informativi [121]. La FROM non si sarebbe conformata alla normativa nell'erronea convinzione di trovarsi nell'impossibilità oggettiva di risalire all'identità degli interessati dal momento che i dati erano stati pseudonimizzati e non era possibile accedere né ai dati identificativi né ai dati di contatto degli interessati.

A nulla sembra valere l'avere ottenuto il parere favorevole del comitato etico territorialmente competente del centro coordinatore e degli altri comitati o l'aver predisposto idonee misure tecniche e organizzative (ad es. il rispetto del principio di minimizzazione, la pseudonimizzazione dei dati clinici inseriti nel database e l'analisi esauriente dei rischi relativi al trattamento dei dati personali). Il Garante, infatti, basandosi su una lettura rigorosa del GDPR [122]

---

[119] Basti guardare alle relazioni che le autorità di controllo sono obbligate a produrre ogni anno ai sensi dell'art. 59 GDPR.

[120] I. RAPISARDA, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?*, in *Eur. dir. priv.*, 2021, fasc. 2, pp. 301-347.

[121] Art. 5, par. 1, lett. a) e art. 14, par. 5, GDPR e art. 6, par. 3, regole deontologiche sulla ricerca scientifica.

[122] Art. 14, par. 5, lett. b), GDPR che fa salve le condizioni e le garanzie previste dall'art. 89, par. 1, GDPR.

e sulle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica [123], ha chiarito che l'eccezione agli obblighi informativi previsti dall'art. 14, par. 5, lett. b), GDPR non esclude che il titolare debba comunque adottare ulteriori misure a tutela degli interessati (ad es. la pubblicazione delle informazioni).

In maniera analoga, nel caso concernente il Progetto *The Health Improvement Network* (THIN) [124], il Garante ha sanzionato la società Thin s.r.l. per aver violato i principi di liceità, correttezza e trasparenza [125]. Anche in questa occasione, il titolare avrebbe commesso un errore nel ritenersi svincolato dalla disciplina, in ragione della natura anonima dei dati raccolti dai medici di base tramite l'utilizzazione del gestionale Medico 2000. Secondo la società Thin erano solo i medici a rivestire il ruolo di titolari e, quindi, a dover informare i pazienti della possibilità che i loro dati potessero essere condivisi, in forma anonima, con terzi per la realizzazione di studi longitudinali volti a migliorare le cure dei pazienti e per scopi di ricerca scientifica epidemiologica e di farmacovigilanza. Per il Garante, invece, è la società Thin che, definendo le modalità di anonimizzazione, agisce da titolare dell'ulteriore trattamento di anonimizzazione, mentre il medico di base assume il ruolo di titolare dei trattamenti di dati personali per fini di cura *ex* art. 9, par. 2, lett. h), GDPR.

Il tema del trattamento ulteriore dei dati personali viene qui esaminato solo incidentalmente. Oltre al caso del progetto THIN, un altro esempio in cui tale questione viene trattata, seppur marginalmente, è quello riguardante lo Studio DB Torax, condotto dall'Azienda Universitaria Integrata di Verona per la creazione di una banca dati finalizzata ad analisi e studi futuri volti al miglioramento delle conoscenze e della pratica clinica nel settore delle patologie del distretto toracico. Pur non riscontrando alcuna violazione in merito alla costituzione del database "DB Torax", le cui basi giuridiche sono state correttamente individuate nel consenso o nell'art. 110 Codice della privacy, il Garante ha rilevato profili di illiceità con riferimento agli eventuali ulteriori trattamenti, di cui non vengono specificate le finalità [126].

---

[123] Art. 6, par. 3, regole deontologiche sulla ricerca scientifica.

[124] Il progetto THIN vede la collaborazione tra diversi Stati membri, tra cui l'Italia e la Francia, al fine di realizzare un database europeo di dati medici anonimizzati raccolti da professionisti sanitari nel corso della loro attività assistenziale per motivi che vanno dalla ricerca epidemiologica alla farmacovigilanza sino all'elaborazione di politiche sulle cure primarie e secondarie. Per ulteriori approfondimenti si rinvia al sito del progetto: https://www.the-health-improvement-network.com/it/#what-is-thin-italian.

[125] Art. 5, par. 1, lett. a) e artt. 9 e 13 GDPR.

[126] Parere n. 238 ai sensi dell'art. 110 del Codice della privacy e dell'art. 36 del Regolamento (doc. web 9791886), del 30 giugno 2022.

Ritenendo gli obiettivi di tali ulteriori trattamenti compatibili con quelli della raccolta, in quanto concernenti le medesime patologie del distretto toracico oggetto dello studio "DB Torax", il titolare ha erroneamente ritenuto sufficiente utilizzare, come condizioni di liceità del trattamento, le due manifestazioni di volontà ottenute al momento della raccolta dei dati: una per il primo trattamento e l'altra, unitamente al parere favorevole del comitato etico territorialmente competente, per la realizzazione di ulteriori progetti di ricerca. Al contrario, secondo il Garante italiano, la fattispecie in questione non è un'ipotesi di trattamenti ulteriori (e compatibili), bensì di trattamenti per i quali, al momento della raccolta, è impossibile individuare le specifiche finalità.

Benché, in questi casi, il considerando 33 GDPR consentirebbe ai titolari di ottenere un consenso ampio, l'Autorità di controllo italiana, facendo propria l'interpretazione del Comitato europeo per la protezione dei dati personali (EDPB) [127], ha chiarito che "non è possibile derogare al requisito della specificità e granularità del consenso" [128] anche in ipotesi del genere. Inoltre, sempre con riferimento alla base giuridica dei trattamenti futuri per finalità non meglio definite, il Garante ha stabilito che qualora i soggetti interessati non possano essere contattati per esprimere un consenso esplicito, occorre soddisfare cumulativamente due condizioni: i) la necessità di rivolgersi al Garante stesso per una previa consultazione che si concluda con un'approvazione del progetto di ricerca; ii) l'ottenimento del parere favorevole sul progetto da parte del comitato etico territorialmente competente. Queste condizioni, per il Garante, rappresenterebbero un "presupposto giuridico equipollente al consenso" [129].

Nel medesimo parere, pur ribadendo che la fattispecie non rientra tra i trattamenti ulteriori dei dati, l'Autorità italiana ha anche colto l'occasione per chiarire il significato della presunzione di non incompatibilità dei trattamenti ulteriori con lo scopo di raccolta iniziale [130]. A questo proposito, richiamando i pareri del Garante europeo per la protezione dei dati personali (EDPS) [131] e

---

[127] Linee guida dell'EDPB n. 05/2020 sul consenso che non ammettono l'esistenza di un "*broad consent*", ma piuttosto di un consenso a fasi progressive o granulare, fornito solamente ad alcuni settori della ricerca o a parti di progetti di ricerca. Tale impostazione deriva dal fatto che il consenso ampio rappresenterebbe un'eccezione al principio di limitazione delle finalità che, secondo il testo del GDPR, non ammette deroghe. Cfr. A. INCERTI, *Il principio di limitazione delle finalità*, in F. BRAVO (a cura di), *Dati personali, Protezione, libera circolazione e governance. I principi*, Pacini Giuridica, Pisa, 2023, pp. 185-230.

[128] Parere n. 238/2022, p. 9.

[129] *Ibid.* p. 10. Come abbiamo visto nella sezione 2.1.1, con la modifica del d.l. n. 19/2024, dall'art. 110 Codice della privacy è stato eliminato il requisito della consultazione preventiva.

[130] Si veda anche il considerando 50 e l'art. 5, par. 1, lett. b), GDPR.

[131] EDPS, *A Preliminary Opinion on Data Protection and Scientific Research*, 2020. In questo parere, l'EDPS fornisce un'interpretazione restrittiva anche dell'eccezione al principio di limitazione della conservazione dei dati (p. 23). In particolare, l'EDPS afferma che "*in*

dell'EDPB [132], è stato precisato che tale presunzione deve essere intesa come ipotesi eccezionale che "non ammette interpretazioni analogiche o estensive", specialmente nel caso di trattamenti di particolari categorie di dati personali [133].

Nel complesso, gli orientamenti espressi dal Garante nei casi analizzati delineano un approccio tendenzialmente improntato alla protezione degli interessati. Da un lato, le deroghe agli obblighi informativi previste dalla disciplina europea sono interpretate in modo restrittivo, rendendone difficile l'applicazione, anche quando il titolare del trattamento abbia ottenuto il parere favorevole del comitato etico competente e abbia adottato adeguate misure tecniche e organizzative. Un analogo rigore si riscontra per il requisito del consenso, che il Garante interpreta in modo da escludere sostanzialmente la possibilità di ricorrere a consensi ampi. Dall'altro, per quanto riguarda il trattamento ulteriore, l'interpretazione stringente del Garante in merito alla presunzione di compatibilità limita la facoltà, da parte dei titolari, di procedere a nuovi trattamenti sul presupposto di liceità di quello originario, anche laddove siano previste adeguate garanzie.

2.2.2. La *Commission Nationale de l'Informatique et des Libertés* e le occasioni per la ricerca

Già nel motto "*[p]rotéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*", collocato in apertura delle relazioni annuali e del sito ufficiale della CNIL, sembra potersi cogliere una differenza nel modo in cui la disciplina sulla protezione dei dati personali viene attuata dall'Autorità francese rispetto al Garante italiano. Tale motto, infatti, esprime in modo sintetico ma efficace la varietà di obiettivi che la CNIL si propone di perseguire nello svolgere la propria attività di *enforcement*: non solo protezione dei dati e delle libertà degli interessati, ma anche promozione dell'innovazione e del progresso tecnologico.

---

principle personal data collected in the commercial or healthcare context, for example, may be further used for scientific research purposes, by the original or a new controller, if appropriate safeguards are in place". Tuttavia, soprattutto quando i dati sono stati raccolti, in un primo momento, per finalità molto differenti o non rientranti nel campo della ricerca scientifica, allora è necessario adoperare il test di compatibilità di cui all'art. 6, par. 4, GDPR. Questa interpretazione viene giustificata sulla base di una lettura distinta dei due requisiti di liceità, da un lato, e del principio di limitazione delle finalità, dall'altro, che prescinde da quanto afferma il considerando 50 GDPR.

[132] Parere dell'EDPB n. 03/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati e documento dell'EDPB in risposta alla domanda di chiarimenti della Commissione europea, 2021.

[133] Parere n. 238/2022, p. 11.

Consultando il sito della CNIL, colpisce il numero di autorizzazioni concesse agli enti pubblici e privati che svolgono attività di ricerca in ambito sanitario [134]. Tra le più recenti, si nota una sintonia di vedute tra i pareri forniti dal CESREES e le osservazioni della CNIL, che raramente nega l'autorizzazione a progetti che hanno ricevuto un riscontro favorevole del CESREES. La struttura delle autorizzazioni segue uno schema preciso e relativamente stabile nel tempo, con una parte centrale in cui la CNIL si concentra su elementi essenziali, quali la ripartizione delle responsabilità tra titolare e responsabili del trattamento, la finalità di interesse pubblico perseguita, la conformità alle norme applicabili, incluse le MR, le categorie di dati e destinatari coinvolti, i termini di conservazione e le misure di sicurezza adottate, le garanzie a tutela dei diritti degli interessati, nonché l'eventuale trasferimento di dati verso Paesi terzi.

Nel caso relativo allo studio condotto dall'*Assistance publique – Hôpitaux de Paris* (AP-HP), con l'aiuto di HDH, ad esempio, la CNIL ha ritenuto il trattamento di dati sanitari effettuato da AP-HP lecito, in quanto necessario per l'adempimento di un interesse pubblico, ai sensi dell'art. 6, par. 1, lett. e), GDPR e art. 9, par. 2, lett. j), GDPR [135]. Il trattamento era, infatti,

---

[134] Tra le più recenti, cfr. *Délibération n° 2023-002 du 12 janvier 2023 autorisant la société ELSAN SAS à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité la constitution d'un entrepôt de données de santé, dénommé "EDS ELSAN". Demande d'autorisation n° 2226980* (creazione di un archivio di dati sanitari da parte del gruppo ELSAN SAS per il miglioramento della qualità delle cure e la realizzazione di studi, ricerche e valutazioni in materia sanitaria, ai sensi dell'art. 6, par. 1, lett. f), e dell'art. 9, par. 2, lett. j), GDPR); *Délibération n° 2023-042 du 27 avril 2023 autorisant la société Clinityx à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur la consommation en France de princeps et biosimilaires anti-TNF alpha, intitulée "Magellan Anti-TNF alpha". Demande d'autorisation n° 923011* (studio svolto da Clinityx, società di consulenza che svolge attività di ricerca in ambito sanitario, servendosi in particolare dei dati del SNDS, ai sensi dell'art. 6, par. 1, lett. f) e dell'art. 9, par. 2, lett. j), GDPR); *Délibération n° 2023-041 du 27 avril 2023 autorisant le Centre hospitalier universitaire de Poitiers et la société Clinityx à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur le taux de réintervention pour complication et le taux de réintervention pour récidive après implantation de bandelettes sous-urétrales au cours d'une chirurgie de l'incontinence urinaire d'effort en distinguant les deux voies d'abord, intitulée "Magellan Mesh". Demande d'autorisation n° 922274* (studio svolto dal Centro Ospedaliero Universitario di Poitiers e Clinityx, per il perseguimento dei loro interessi legittimi, ai sensi dell'art. 6, par. 1, lett. f) e dell'art. 9, par. 2, lett. j), GDPR). Per ulteriori esempi, si rimanda alla sezione dedicata del sito della CNIL: https://www.cnil.fr/fr/deliberations.

[135] *Délibération n. 2023-028 du 23 mars 2023 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur l'épidémiologie et les parcours de soins des enfants présentant des variations du développement génital, intitulée "VarGen". Demande d'autorisation n. 922276*.

finalizzato alla realizzazione dello studio "VarGen", volto ad analizzare l'epidemiologia e i percorsi di cura dei bambini con variazioni nello sviluppo genitale, nell'ambito dell'elaborazione di un rapporto che, in base alla legge francese sulla bioetica del 2021, il Governo è tenuto a presentare al Parlamento per riferire sull'attività e sul funzionamento dei centri di riferimento competenti per le malattie rare.

Oltre ad autorizzare l'uso primario dei dati provenienti dal *Système national des données de santé* (SNDS), la CNIL ha approvato anche il riutilizzo dei dati della *Banque nationale de données maladies rares* (BNDMR), per via della conformità con il quadro previsto dalla metodologia di riferimento MR-004. Per quanto riguarda poi l'adempimento degli oneri informativi, la CNIL ha stabilito che l'eccezione al principio dell'informazione individuale in caso di raccolta indiretta, ai sensi dell'art. 14, par. 5, lett. b), GDPR, può essere soddisfatta attraverso la diffusione delle informazioni collettive nel sito web del titolare, l'apposizione di poster nei centri di riferimento per le malattie rare e nei relativi siti web, nonché la registrazione dello studio nel portale trasparenza di HDH.

Considerazioni analoghe sono state formulate anche in relazione a un ulteriore studio condotto dallo stesso titolare (AP-HP), sempre in collaborazione con HDH, per lo sviluppo e la validazione di algoritmi di targeting, capaci di identificare nel SNDS le malattie rare autoimmuni e autoinfiammatorie sistemiche (studio "EMIR-Algo"), nell'adempimento della missione di interesse pubblico affidata a AP-HP, in conformità degli artt. 6, par. 1, lett. e) e 9, par. 2, lett. j), GDPR [136]. Rispetto ai rilievi sollevati con riferimento allo studio VerGen, l'unica osservazione aggiuntiva della CNIL concerne la necessità per il titolare di effettuare uno studio di rischio prima di qualsiasi pubblicazione *open source* dei modelli sviluppati con metodi di *machine learning*, per verificare che non sia possibile estrarre dati personali o dedurre la presenza di una persona nel dataset di addestramento.

Un ultimo caso illustrativo dell'approccio della CNIL riguardo all'uso primario e secondario dei dati è la richiesta di accesso ai dati della banca dati *Programme de médicalisation des systèmes d'information* (PMSI) da parte di una società di stampa specializzata nel settore sanitario (APM). In questa occasione, la CNIL, allineandosi al parere fornito dal CESREES, ha autorizzato la richiesta, riconoscendo la finalità di interesse pubblico alla base dell'attività di trattamento [137]. APM intendeva infatti analizzare, mediante i dati nazionali

---

[136] *Délibération n. 2023-029 du 23 mars 2023 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur l'épidémiologie des maladies inflammatoires systémiques rares en France, intitulée "EMIR-Algo". Demande d'autorisation n. 922278*.

[137] *Délibération n. 2023-020 du 9 mars 2023 portant décision unique et autorisant la société "APM International" à mettre en œuvre des traitements automatisés à des fins de*

contenuti nella banca PMSI, l'evoluzione del sistema ospedaliero francese e valutare l'efficacia delle politiche sanitarie adottate.

Di segno opposto è stato, invece, l'esito di un caso precedente riguardante la richiesta di autorizzazione avanzata dalla società editrice del settimanale *Le Point* (SEBDO) per accedere alla medesima banca dati PMSI. Tale accesso era stato negato in quanto la CNIL, allineandosi ancora una volta al parere del CESREES, non aveva ritenuto l'interesse pubblico fatto valere sufficientemente caratterizzato. Secondo l'Autorità, l'obiettivo perseguito da SEBDO, ovvero la redazione di una classifica degli ospedali e delle cliniche francesi, non poteva essere equiparato a un'attività di ricerca condotta da un organismo pubblico o accademico, ma costituiva piuttosto un'elaborazione giornalistica, peraltro viziata da rilevanti carenze metodologiche, finalizzata a informare il pubblico sulla qualità delle cure fornite dalle strutture sanitarie [138].

Dalle decisioni prese in esame emerge come la CNIL, pur operando in un quadro normativo certamente diverso da quello del Garante, abbia adottato un approccio generalmente più favorevole al trattamento dei dati personali. Tale orientamento si riflette in una prassi applicativa che ricerca un equilibrio tra la tutela dei diritti degli interessati e le esigenze legittime dei titolari del trattamento. Nelle proprie autorizzazioni, infatti, la CNIL si attiene in modo rigoroso al dettato normativo, evitando di introdurre requisiti ulteriori rispetto a quelli previsti dalla legge, e fonda le sue decisioni su un'analisi puntuale e contestuale degli elementi fattuali, scongiurando ogni applicazione automatica o formalistica della disciplina.

A questo si aggiunge l'impegno costante dell'Autorità francese nell'adozione e nell'aggiornamento delle MR che – come ricordato nella sezione 2.1.2 – consentono al titolare di trattare i dati senza necessità di autorizzazione preventiva, ma semplicemente mediante una dichiarazione di conformità alla metodologia applicabile. Oltre a quelle già esistenti, come la MR-004 per gli studi che riutilizzano i dati sanitari alla luce di un interesse pubblico e le MR-

---

recherche, d'étude et d'évaluation dans le domaine de la santé nécessitant un accès aux données nationales du programme de médicalisation des systèmes d'information (PMSI). Saisine n. 922297.

[138] Il ragionamento della CNIL è stato poi avallato dal Conseil d'État che ha ritenuto che il rifiuto della CNIL a concedere l'autorizzazione a SEBDO non costituisse una violazione della libertà di informazione sull'attività di cura. L'Autorità francese, infatti, aveva esaminato correttamente la domanda, prestando particolare attenzione a "*à la qualité d'organisme de presse de la société requérante et, partant, à la nécessité, au regard de la liberté de la presse, d'assurer l'accès des journalistes aux sources utiles à leurs investigations, pour autant qu'est garantie la qualité de l'information délivrée au public, la SEBDO n'est pas fondée à soutenir que le refus d'autorisation qui lui a été opposé porte une atteinte disproportionnée à la liberté de la presse et à la liberté d'expression garanties par l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales*" (Conseil d'État, 10ème-9ème chambres réunies, 30 juin 2023, 469964, par. 15).

005 e 006 per gli studi che richiedono l'accesso ai dati PMSI da parte di strutture sanitarie o produttori di prodotti sanitari, la CNIL ha recentemente introdotto due nuove MR (MR-007 e MR-008) che agevolano l'accesso ai dati dello SNDS da parte di enti pubblici e privati, ad eccezione degli assicuratori [139]. In un'ottica di ulteriore semplificazione, la CNIL ha inoltre definito un sistema di riferimento specifico per la creazione di *data warehouse* in ambito sanitario [140], elaborando una *check-list* di conformità destinata a guidare i titolari nella progettazione e nella gestione di architetture dati destinate alla ricerca, alla valutazione e allo studio nel settore della sanità [141].

2.2.3. Gli elementi di differenziazione tra le prassi amministrative delle autorità di controllo e i correttivi presenti nel GDPR

Nonostante i casi analizzati presentino elementi fattuali e giuridici non perfettamente coincidenti, è comunque possibile sottolineare alcune differenze rilevanti nel modo in cui le autorità di controllo italiana e francese applicano il GDPR e la disciplina nazionale di attuazione. Innanzitutto, si osserva che il Garante, a differenza della CNIL, non sembra tenere particolarmente in considerazione i rilievi positivi del comitato etico competente [142]. Di conseguenza, ottenere il nulla osta da parte del comitato etico solitamente non appare, di per sé, sufficiente per il titolare a ottenere l'approvazione del proprio progetto di ricerca, né a beneficiare di un alleggerimento degli adempimenti da compiere (ad es. gli oneri informativi nei confronti degli interessati).

---

[139] Délibération n 2023-082 du 20 juillet 2023 portant homologation d'une méthodologie de référence relative aux traitements de données de la base principale du Système national des données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissant dans le cadre de leur mission d'intérêt public (MR-007); Délibération n 2023-083 du 20 juillet 2023 portant homologation d'une méthodologie de référence relative aux traitements de données de la base principale du Système national des données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissant dans le cadre de leurs intérêts légitimes (MR-008). Queste deliberazioni contengono una serie di innovazioni rispetto a quelle già esistenti e, in particolare, MR-005 e MR-006. Le novità principali riguardano le finalità che possono giustificare l'uso dei dati (ad es. oltre a quelle previste da MR-005, viene aggiunta la realizzazione di studi di fattibilità per ricerche che coinvolgono o meno la persona umana); l'ottenimento del parere del comitato etico; l'obbligo di inviare alla CNIL, ogni tre anni, una relazione sulle pratiche e sull'uso dei loro trattamenti.

[140] *Délibération n. 2021-118 du 7 octobre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé*.

[141] https://www.cnil.fr/sites/cnil/files/atoms/files/check-list_de_conformite_referentiel-donnes-sante.pdf.

[142] Si rinvia al caso relativo al Studio "DB Torax" e a quello sullo studio ERNEST 2.0.

Inoltre, per quanto riguarda il fondamento giuridico, la scelta del Garante di adottare un'interpretazione rigorosa del consenso, in linea con le indicazioni fornite dall'EDPB, escludendo sostanzialmente la possibilità di concepirlo in senso ampio, richiede ai titolari di avvalersi delle ipotesi derogatorie all'obbligo di ottenere il consenso *ex* artt. 110-110-*bis* Codice della privacy. Queste deroghe, tuttavia, impongono al titolare di avviare la procedura di consultazione preventiva (pre-modifica ad opera del d.l. n. 19/2024) o di osservare le garanzie adottate dal Garante *ex* art. 106, par. 2, lett. d), Codice della privacy, nelle quali il requisito del consenso resta comunque centrale [143]. Non è così invece nelle MR della CNIL, il cui rispetto non richiede adempimenti particolarmente gravosi ai titolari che trattano dati per fini di ricerca scientifica sulla base di un interesse pubblico o di un interesse legittimo.

In linea generale, anche se il contesto normativo in cui le autorità di controllo italiana e francese operano limita certamente la loro discrezionalità, è possibile rilevare che Garante italiano, diversamente dalla CNIL, tende a privilegiare in modo marcato – talvolta eccessivo – la tutela dell'autodeterminazione informativa degli interessati. Questo orientamento risulta problematico sotto più profili, tanto a livello nazionale quanto transfrontaliero. Sul piano interno, c'è il rischio di minare la capacità dell'Italia di progredire nell'ambito della ricerca. Ciò appare ancor più vero se si considera il passaggio da un approccio teoria-centrico, dove "l'utilità dei dati sta nel funzionare come prova della plausibilità di una ipotesi già data, confermando così asserzioni che i ricercatori interpretano come nuove scoperte", a uno dato-centrico, in cui "i dati sono visti come entità pubbliche che hanno valore scientifico indipendentemente dal loro ruolo di prova per una determinata ipotesi e che possono essere interpretati in modi diversi a seconda delle abilità e degli interessi dei ricercatori che li analizzano" [144].

Sul piano europeo, la frammentazione delle prassi tra le autorità di controllo – spesso alimentata da divergenze normative a livello nazionale – rischia di compromettere la realizzazione della libera circolazione dei dati personali, che tali autorità dovrebbero facilitare [145]. Come anticipato nella sezione 2.1.3 con riguardo alle differenze tra le discipline nazionali, questa disomogeneità costituisce un ostacolo concreto alla conduzione di progetti di

---

[143] Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica, par. 5.3; prescrizioni relative al trattamento dei dati genetici, parr. 4.5 e 4.11.2; art. 8 regole deontologiche sulla ricerca scientifica.

[144] S. LEONELLI, *op. cit*., 2018, pp. 28-29.

[145] Art. 51, par. 1, GDPR. Si rimanda anche al considerando 123 e agli artt. 51-58 GDPR. Sul punto, cfr. sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms*, punti 45-46; del 9 marzo 2010, causa C-518/07, *Commissione c. Germania*, ECLI:EU:C:2010:12, punto 30.

ricerca internazionale [146], portando ad esempio a valutazioni strategiche rispetto ai partner da includere nei consorzi [147]. Secondo il meccanismo dello sportello unico di cui all'art. 60 GDPR [148], infatti, i casi transfrontalieri devono essere decisi dall'autorità di controllo dello Stato membro in cui il titolare ha il proprio stabilimento principale [149]. Di conseguenza, è plausibile che si verifichino pratiche di *forum shopping* verso quegli Stati dove le autorità di controllo hanno un approccio maggiormente *research-friendly* [150], come già avviene, in altri settori, per Stati quali Irlanda e Lussemburgo, scelti da molte aziende tecnologiche (ad es. Meta, Instagram e Whatsapp) per registrare la propria sede [151], anche in ragione dell'atteggiamento permissivo delle rispettive autorità di controllo [152].

A questo proposito, gli strumenti previsti dal GDPR per assicurare

---

[146] Lo studio Ernest 2.0 e il progetto THIN ne sono un esempio. Il primo, infatti, consiste in uno studio multicentrico, osservazionale e retrospettivo, che si propone di analizzare i dati clinici archiviati presso i centri partecipanti (sei con sede in Italia e uno in Spagna) per esaminare il tasso di mortalità dei pazienti affetti da mielofibrosi coinvolti nel progetto ERNEST nell'arco di tempo tra il 2014 e il 2018. Analogamente, il progetto THIN vede la collaborazione tra diversi Stati membri al fine di realizzare un database europeo di dati medici anonimizzati raccolti da professionisti sanitari nel corso della loro attività di assistenza per motivi che vanno dalla ricerca epidemiologica alla farmacovigilanza sino all'elaborazione di politiche sulle cure primarie e secondarie.

[147] E.B. VAN VEEN, *op. cit.*, 2018, p. 75.

[148] In sintesi, lo sportello unico consiste in un processo decisionale consensuale, fondato su uno scambio di informazioni nell'ottica della leale cooperazione che rappresenta la chiave di volta dell'intero sistema (sentenza della Corte del 15 giugno 2021, causa C-645/19, *Facebook Ireland e a.*, ECLI:EU:C:2021:483). Sul punto si rimanda alle linee guida dell'EDPB n. 02/2022 sull'applicazione dell'art. 60 del GDPR.

[149] Art. 56 GDPR.

[150] K. PORMEISTER, *op. cit*., 2017, p. 146.

[151] Nel 2021, il Parlamento europeo ha espresso la sua preoccupazione "per via del fatto che l'autorità di protezione dei dati irlandese chiude, in generale, la maggior parte dei casi con una composizione della controversia anziché con una sanzione, e che i casi deferiti all'Irlanda nel 2018 non hanno nemmeno raggiunto la fase di un progetto di decisione". Cfr. Risoluzione del Parlamento sulla relazione di valutazione della Commissione concernente l'attuazione del GDPR, p. 8. A questo proposito, però, occorre ricordare che, di recente, l'EDPB ha adottato delle linee guida n. 06/2022 sull'attuazione della pratica delle composizioni amichevoli.

[152] Oltre all'approccio più o meno permissivo delle autorità di controllo, tra i fattori che possono influenzare la scelta del luogo di stabilimento del titolare rientra anche il contesto regolatorio dello Stato membro, ad esempio in materia di concorrenza o di politiche di deregolamentazione. In questo senso, normative meno restrittive o maggiormente orientate a promuovere l'attrattività economica possono contribuire a dinamiche simili a quelle osservate in altri settori, riflettendo effetti distorsivi della frammentazione normativa, che il diritto dell'Unione mira a ridurre, ma che permangono nonostante gli strumenti di armonizzazione previsti.

un'applicazione coerente e omogenea della disciplina non paiono essere risolutivi [153]. Sin dalla prima valutazione dell'applicazione del GDPR nel 2020, la Commissione ha rilevato che le autorità di controllo non si erano ancora avvalse di strumenti come le operazioni congiunte [154]. Inoltre, secondo la Commissione, gli Stati non hanno sfruttato appieno le possibilità per promuovere una maggiore armonizzazione tramite il meccanismo di coerenza [155], ad esempio, con riferimento agli elenchi nazionali dei trattamenti che richiedono lo svolgimento di una DPIA [156]. Come si vedrà più avanti, proprio queste

[153] Per un'analisi più approfondita sul punto, si rinvia, *inter alia*, a G. GENTILE, O. LYNSKEY, *Deficient by Design? The Transnational Enforcement of the GDPR*, in *ICLQ*, 2022, vol. 71, n. 4, pp. 799-830 e A. FIORENTINI, *Alla ricerca di un punto di equilibrio tra autonomia istituzionale ed effettività del diritto per le forme di integrazione amministrativa nel settore digitale*, in *Quaderni AISDUE*, 2023, n. 29, pp. 666-668.

[154] Art. 62 GDPR.

[155] Secondo l'art. 64 GDPR, l'EDPB è tenuto a emettere un parere quando un'autorità di controllo intende adottare delle misure volte, tra le altre cose, a stabilire un elenco di trattamenti soggetti al requisito della DPIA e determinare clausole tipo di protezione dei dati. Inoltre, le autorità di controllo possono richiedere tale parere su questioni di applicazione generale o che producono effetti transfrontalieri.

[156] Artt. 35, par. 4, e 64, par. 1, lett. a), GDPR. In ottemperanza a tale obbligo, l'autorità di controllo francese ha predisposto un elenco (non esaustivo) delle tipologie di trattamenti per i quali ritiene obbligatorio effettuare una DPIA (ad es. trattamenti di dati genetici riferiti a persone vulnerabili) e di quelli per cui, invece, non è necessaria (https://www.cnil.fr/fr/listes-des-traitements-pour-lesquels-une-aipd-est-requise-ou-non). In modo analogo, anche l'autorità italiana ha adottato un proprio elenco, sul quale l'EDPB si è espresso con il parere n. 12/2018. Da tale parere emerge l'importanza di valutare in concreto se un determinato trattamento – anche qualora riguardi dati appartenenti a categorie particolari, come dati biometrici o genetici – comporti effettivamente un rischio elevato per i diritti e le libertà delle persone fisiche (parere n. 12/2018 sull'elenco delle tipologie di trattamenti soggetti a DPIA ai sensi dell'art. 35, par. 4, GDPR, adottato l'11 ottobre 2018, n. 467 [doc. web n. 9058979]). L'approccio dell'EDPB si pone in continuità con quanto già affermato dal Gruppo di Lavoro *ex* art. 29 (WP), le cui linee guida individuano nove criteri indicativi dei trattamenti potenzialmente in grado di comportare un rischio elevato, tra cui quelli che coinvolgono soggetti vulnerabili o il monitoraggio sistematico delle persone (linee guida WP sulla valutazione d'impatto e sulla determinazione dell'eventuale "rischio elevato" ai sensi del regolamento (UE) 2016/679, 2017, recepite dall'EDPB nel 2018, WP 248 rev. 01). L'EDPB precisa inoltre che, anche quando un trattamento soddisfa più di due criteri tra quelli individuati dal WP, il titolare può comunque evitare di effettuare una DPIA, purché dimostri e documenti le ragioni per cui essa non risulta necessaria, includendo il punto di vista del DPO, se designato. Tale indicazione è stata recepita dalla CNIL nelle proprie linee guida in materia di DPIA (https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037559518). Da ultimo, va segnalato che, nel tentativo di superare l'attuale frammentazione, la proposta di regolamento *Digital Omnibus* attribuisce all'EDPB il compito di elaborare liste dei trattamenti che richiedono o non richiedono una DPIA, nonché metodologie uniformi per svolgerla. Tali liste e metodologie verranno poi adottate, tramite atto di esecuzione, dalla Commissione (art. 3, par. 9, proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE)

criticità hanno contribuito ad avviare un processo di riforma delle disposizioni di natura procedurale del GDPR.

3. Verso un'applicazione del GDPR maggiormente uniforme alla luce delle novità introdotte dallo spazio europeo dei dati sanitari

Anche se circoscritta a un ambito specifico, l'analisi condotta nella sezione precedente mostra come l'applicazione del GDPR abbia generato – e continui a generare – un quadro fortemente frammentato nell'Unione, sia a livello normativo sia, di riflesso, a livello di prassi amministrative. Tale quadro appare oggi anacronistico rispetto agli obiettivi espressi dalla Commissione nella Strategia europea per i dati del 2020 [157], come la costruzione di spazi comuni europei in settori ritenuti di importanza strategica (*in primis*, lo EHDS). Non sembra ormai più procrastinabile, quindi, il momento di compiere delle scelte che vadano nella direzione di superare gli ostacoli alla libera circolazione dei dati personali derivanti da un'applicazione eterogenea delle norme del GDPR, assicurando una maggiore disponibilità di dati nell'Unione.

Con la proposta di EHDS, questa esigenza ha trovato una prima risposta concreta in un quadro normativo che mira, tra le altre cose, a promuovere lo scambio di dati sanitari elettronici per finalità primarie e secondarie, non solo all'interno dei singoli Stati membri – come illustrato nel capitolo 3 – ma anche tra di essi.

Per quanto riguarda la circolazione dei dati per finalità di assistenza sanitaria, lo EHDS richiede, innanzitutto, che i servizi di delega nazionali siano interoperabili tra gli Stati membri [158]. Ciò significa, per esempio, che un anziano residente in Italia può autorizzare il figlio, che vive in un altro Stato membro, ad accedere ai propri dati sanitari senza incontrare ostacoli tecnici. Sempre in questa prospettiva, viene introdotto l'obbligo per gli Stati membri di adottare il formato europeo di scambio delle cartelle cliniche

---

2018/1725, (UE) 2023/2854 e delle 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 della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025).

[157] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati, COM/2020/66 final, del 19 febbraio 2020.

[158] Art. 4, parr. 3-4, EHDS. Questa disposizione incarica la Commissione di stabilire, tramite l'adozione di atti di esecuzione, le specifiche tecniche necessarie per assicurare l'interoperabilità tra i sistemi di delega.

elettroniche [159], così da garantire ai cittadini dell'Unione la possibilità di ottenere una copia dei loro dati sanitari ovunque essi si trovino [160] e di richiedere che un fornitore di assistenza sanitaria trasmetta tali dati a un fornitore situato in un altro Stato membro [161]. Grazie a tale formato, il destinatario (ad es. un professionista sanitario o un farmacista) viene posto nelle condizioni di poter leggere i dati ricevuti e utilizzarli per erogare assistenza sanitaria o dispensare farmaci [162].

Nella pratica, i fornitori di assistenza sanitaria che effettuano scambi di dati sanitari elettronici e le farmacie che dispensano le prescrizioni elettroniche rilasciate da altri Stati membri dovranno collegarsi ai punti di contatto nazionali, designati in seno alle autorità di sanità digitale e connessi a loro volta alla piattaforma centrale di interoperabilità nell'ambito dell'infrastruttura transfrontaliera MyHealth@EU [163]. La partecipazione a tale infrastruttura potrà essere autorizzata, a determinate condizioni, anche ai punti di contatto di Paesi terzi in modo da garantire la continuità delle cure, specialmente per le popolazioni mobili transfrontaliere con Paesi terzi confinanti, i paesi candidati e l'associazione dei paesi e territori d'oltremare [164].

Oltre a offrire servizi volti a facilitare lo scambio di dati tra i diversi punti di contatto nazionale, garantendo così alle persone fisiche di esercitare il loro diritto ad accedere a cure di qualità, come stabilito dal regolamento (CE) 883/2004 e dalla direttiva 2011/24/UE, MyHealth@Data è stata concepita anche per fornire servizi supplementari per "agevolare la telemedicina, la sanità mobile, l'accesso da parte delle persone fisiche ai dati sanitari tradotti e lo scambio o la verifica di certificati sanitari, […] i servizi e le applicazioni interoperabili di sanità digitale" [165]. In aggiunta, qualora MyHealth@EU non sia in grado di supportare alcuni servizi, come lo scambio di informazioni sui piani di vaccinazione o il tracciamento dei contatti per il contenimento di malattie infettive, la Commissione può, tramite atti di esecuzione, stabilire un collegamento con altre infrastrutture nei campi della salute, dell'assistenza e

[159] Art. 15 EHDS. Come ricordato al capitolo 1, sezione 4.3, lo EHDS definisce il formato europeo di scambio delle cartelle cliniche elettroniche quale formato strutturato, di uso comune e leggibile da un dispositivo automatico che consente la trasmissione di dati sanitari elettronici personali (ad es. prescrizioni e dispensazioni elettroniche) tra applicazioni software, dispositivi e prestatori di assistenza sanitaria diversi.

[160] Art. 3 EHDS.

[161] Art. 7 EHDS.

[162] Considerando 26 EHDS.

[163] Art. 23 EHDS.

[164] Art. 24, par. 3, e considerando 35 EHDS.

[165] Art. 24 EHDS.

della sicurezza sociale (ad es. il sistema di gestione dei dati clinici dei pazienti) [166].

Passando all'uso secondario dei dati sanitari elettronici, la loro circolazione viene favorita tramite la previsione di una procedura comune per le domande di accesso ai dati sanitari e le richieste di dati sanitari, gestita dagli organismi responsabili dell'accesso ai dati oppure dalla Commissione tramite il servizio di accesso ai dati dell'Unione [167]. Inoltre, specularmente a quanto stabilito per l'uso primario, lo EHDS prevede l'istituzione dell'infrastruttura HealthData@EU che collega i punti di contatto nazionali designati da ciascuno Stato membro come *gateway* organizzativo e tecnico per la condivisione dei dati sanitari per uso secondario in contesti transfrontalieri [168].

In pratica, dunque, quando un soggetto intende accedere ai dati sanitari da titolari stabiliti in più di uno Stato membro, egli non deve presentare una domanda a ciascuno dei titolari, bensì un'unica domanda di accesso ai dati (*principle of "single application"*) [169] all'organismo responsabile per l'accesso ai dati dello stabilimento principale del richiedente o di uno dei titolari, oppure tramite i servizi forniti dalla Commissione nell'ambito dell'infrastruttura HealthData@EU [170]. Nel caso in cui i dati che si intende ottenere sono nella disponibilità di istituzioni, organi, organismi e agenzie dell'Unione, è la Commissione, e non l'organismo per l'accesso ai dati, che si occupa di gestire le domande tramite il servizio di accesso ai dati dell'Unione che rappresenta il punto di contatto per queste situazioni in HealthData@EU [171].

---

[166] Art. 24, par. 2, e considerando 35 EHDS. Il *Clinical Patient Management System* è stato sviluppato dalla Commissione per facilitare la collaborazione a distanza tra gli operatori sanitari delle reti di riferimento europee (decisione di esecuzione (UE) 2019/1269 della Commissione del 26 luglio 2019 che modifica la decisione di esecuzione 2014/287/UE della Commissione che stabilisce criteri per l'istituzione e la valutazione delle reti di riferimento europee e dei loro membri e per agevolare lo scambio di informazioni e competenze in relazione all'istituzione e alla valutazione di tali reti).

[167] Per un approfondimento su questi aspetti, si rinvia a quanto già descritto nel capitolo 3, sezione 3.2.2, relativamente ai sistemi di governance dei dati.

[168] Art. 52 EHDS.

[169] Considerando 83 EHDS.

[170] Art. 67, par. 3, EHDS. Regole parzialmente differenti sono previste in caso di richiesta di accesso a registri o dataset transfrontalieri (ad es. i registri delle reti di riferimento europee per malattie rare), dove l'organismo responsabile a decidere sulla domanda di accesso ai dati o la richiesta di dati è quello dello Stato membro in cui il titolare è registrato oppure, qualora vi siano dei contitolari, quello dello Stato membro in cui uno dei contitolari è stabilito. Inoltre, quando i registri o i dataset sono organizzati in un unico network di registri o dataset a livello sovranazionale, l'organismo responsabile è quello dello Stato membro in cui il coordinatore del network è situato (art. 76 EHDS).

[171] Artt. 56 e 75 EHDS.

Nel decidere se autorizzare una domanda di accesso ai dati o se rispondere a una richiesta, gli organismi responsabili dell'accesso ai dati o, eventualmente, la Commissione devono compiere un'attenta valutazione relativa al soddisfacimento di determinate condizioni. Tale valutazione, quindi, non è lasciata completamente alla loro discrezionalità, ma deve avvenire sulla base dei requisiti stabiliti dallo EHDS [172]. Inoltre, al fine di armonizzare gli approcci degli organismi responsabili e ridurre gli oneri amministrativi per i richiedenti, lo EHDS attribuisce alla Commissione il compito di adottare atti di esecuzione che stabiliscono, ad esempio, *templates* specifici per effettuare la domanda di accesso ai dati o la richiesta di dati *ex* artt. 45 e 47 EHDS [173].

In aggiunta, per ampliare le opportunità di accesso e condivisione dei dati a livello europeo – come già avviene nell'ambito di MyHealth@EU – lo EHDS attribuisce alla Commissione il compito di autorizzare, mediante atti di esecuzione, la partecipazione a HealthData@EU di ulteriori soggetti, tra cui infrastrutture di ricerca in ambito sanitario (ad es. i consorzi per le infrastrutture di ricerca europee o digitali), nonché strutture analoghe quali lo *European Strategy Forum for Research Infrastructure* (ESFRI) e lo *European Open Science Cloud* (EOSC), fino a includere anche i punti di contatto dei Paesi terzi [174]. La Commissione può anche fornire, oltre ai servizi di scambio dei dati, ulteriori strumenti finalizzati a facilitare la conoscibilità dei dati disponibili (ad es. la creazione e il mantenimento di cataloghi dei dati), nonché promuovere l'interoperabilità attraverso l'istituzione di ambienti sicuri per il trattamento e l'analisi dei dati provenienti da diverse infrastrutture nazionali o da altri spazi europei comuni di dati [175].

Ai fini della presente analisi risultano particolarmente rilevanti le precisazioni introdotte nel corso dell'iter legislativo dello EHDS – anche su impulso dell'EDPB e dell'EDPS [176] – in merito alle basi giuridiche su cui devono fondarsi i trattamenti di dati sanitari elettronici personali necessari per lo svolgimento delle attività previste nell'ambito del nuovo spazio europeo dei dati sanitari. L'intento è evitare che la scelta della base giuridica venga lasciata alla discrezionalità degli Stati membri, come avvenuto con il GDPR, con il rischio di soluzioni normative eterogenee e disomogeneità applicative che potrebbero gravare in modo differente su chi fornisce o utilizza i dati all'interno dello EHDS.

---

[172] Artt. 68 e 69, par. 3, EHDS.

[173] Art. 70 e considerando 73 EHDS.

[174] Art. 75, parr. 4-5 e considerando 80 EHDS.

[175] Artt. 75, parr. 8, 9 e 11, e considerando 80 EHDS.

[176] Parere congiunto di EDPB e EDPS n. 03/2022.

Con riferimento all'uso primario, i trattamenti necessari per offrire servizi di accesso ai dati sanitari, in quanto finalizzati all'esecuzione di compiti di interesse pubblico, devono fondarsi sugli artt. 6, par. 1, lett. e), e 9, par. 2, lett. g) o h), GDPR [177], a seconda che si tratti di accesso ai dati da parte dei pazienti o dei professionisti sanitari [178]. Lo EHDS prevede, in conformità all'art. 9, par. 2, lett. g) e h), GDPR, adeguate garanzie per il trattamento dei dati, tra cui misure relative ai sistemi di identificazione elettronica e alla trasparenza nella raccolta e nell'uso dei dati. Gli artt. 6, par. 1, lett. e) e 9, par. 2, lett. h), GDPR costituiscono poi le condizioni di liceità per lo scambio transfrontaliero di dati tramite l'infrastruttura MyHealth@EU, nella quale la Commissione agisce come responsabile del trattamento ai sensi dell'art. 4, n. 8, GDPR, mentre i punti di contatto nazionali assumono il ruolo di contitolari del trattamento *ex* art. 26 GDPR [179].

Per quanto riguarda invece l'uso secondario, la base giuridica dipende dalla natura del soggetto che effettua il trattamento. Qualora si tratti del titolare dei dati, obbligato dallo EHDS a metterli a disposizione per finalità specifiche [180], il trattamento trova fondamento negli artt. 6, par. 1, lett. c), e 9, par. 2, lett. i) e j), GDPR [181]. Al contrario, l'organismo responsabile dell'accesso ai dati, chiamato a svolgere funzioni di interesse pubblico come la gestione degli ambienti sicuri di trattamento, opera sulla base degli artt. 6, par. 1, lett. e), e 9, par. 2, lett. g)-j), GDPR. Infine, gli utenti sono liberi di individuare una base giuridica *ex* GDPR, ma qualora fondino il proprio trattamento su un interesse pubblico o su un interesse legittimo, ai sensi dell'art. 6, par. 1, lett. e) o f), GDPR [182], lo EHDS fornisce, ai sensi dell'art. 9, par. 2, GDPR, le

---

[177] L'art. 6, par. 1, lett. e), GDPR rappresenta la base giuridica per i trattamenti di dati personali necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri cui è investito il titolare. L'art. 9, par. 2, lett. g) e h), GDPR, invece, costituisce la condizione di liceità per i trattamenti di dati sensibili necessari, rispettivamente, per motivi di interesse pubblico rilevante e per finalità di medicina preventiva o medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale o gestione dei sistemi e servizi sanitari o sociali.

[178] Considerando 19 e 20 EHDS.

[179] Considerando 34 EHDS.

[180] Art. 51 EHDS.

[181] L'art. 6, par. 1, lett. c), GDPR permette di giustificare trattamenti di dati personali necessari per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, mentre l'art. 9, par. 1, lett. i) e j), GDPR rende leciti trattamenti di dati sanitari necessari rispettivamente per motivi di interesse pubblico nel settore della sanità (ad es. la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici), e per fini di archiviazione nell'interesse pubblico, statistici, di ricerca scientifica o storica.

[182] Se l'art. 6, par. 1, lett. e), GDPR rappresenta la base giuridica per i trattamenti di dati personali necessari per motivi di interesse pubblico, l'art. 6, par. 1, lett. f), GDPR costituisce

garanzie ritenute necessarie e sufficienti per il loro svolgimento, tra cui la previsione di finalità chiaramente definite, un sistema di governance affidabile e ambienti sicuri per il trattamento dei dati.

Tali misure dovrebbero impedire agli Stati membri di introdurre ulteriori condizioni o restrizioni ai sensi dell'art. 9, par. 4, GDPR, come l'obbligo di ottenere il consenso dell'interessato o l'adozione di misure nazionali supplementari [183]. In base a tale articolo, ad esempio, il Codice della privacy prevede l'intervento dell'autorità di controllo italiana per l'adozione di specifiche misure di garanzia [184] e la fissazione di regole deontologiche [185]. Similmente, in Francia, la LIL ha attribuito alla CNIL il compito di prescrivere misure supplementari, in particolare di natura tecnica ed organizzativa [186].

Oltre a chiarire i presupposti di liceità dei trattamenti di dati sanitari elettronici per finalità primarie e secondarie, lo EHDS specifica anche i ruoli ricoperti, ai sensi del GDPR, dai diversi attori coinvolti [187]. Il *data holder* deve considerarsi titolare del trattamento *ex* art. 4, n. 7, GDPR quando rende disponibili i dati richiesti all'organismo per l'accesso ai dati. Quest'ultimo, invece, può essere: i) titolare del trattamento *ex* art. 4, n. 7, GDPR quando prepara i dati e li rende disponibili all'utente; o ii) responsabile del trattamento *ex* art. 4, n. 8, GDPR quando tratta i dati per conto dell'utente all'interno dell'ambiente di trattamento sicuro o li elabora per generare una risposta a una richiesta di dati. L'utente, dall'altra parte, è titolare del trattamento *ex* art. 4, n. 7, GDPR nel caso in cui utilizzi i dati pseudonimizzati nell'ambiente sicuro di trattamento sulla base dell'autorizzazione ricevuta dall'organismo per l'accesso ai dati.

Da quanto precede sembra dunque possibile affermare che la libera circolazione dei dati personali possa finalmente conoscere un nuovo impulso, almeno in ambito sanitario, grazie allo EHDS che interviene su un duplice livello: da un lato, introduce requisiti di interoperabilità per i servizi di delega e meccanismi specifici per l'accesso e la condivisione dei dati anche a livello

---

la condizione di liceità per i trattamenti necessari al perseguimento dell'interesse legittimo del titolare del trattamento o di terzi, a meno che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

[183] Considerando 52 EHDS.

[184] Art. 2-*septies* Codice della privacy che, oltre a richiamare le condizioni di liceità di cui all'art. 9, par. 2, GDPR, inserisce altre condizioni per la legittimità del trattamento, tra cui il rispetto e la conformità delle misure di garanzia, adottate a cadenza biennale, dal Garante. Secondo Rapisarda, le misure di garanzia di cui all'art. 2-*septies* Codice della privacy, da un punto di vista contenutistico non si discostano "molto dalle autorizzazioni generali di cui all'art. 110-*bis*" (I. RAPISARDA, *op. cit.*, 2021, p. 324).

[185] Art. 2-*quater* Codice della privacy.

[186] Art. 8, par. 1, punto 2, lett. c), LIL.

[187] Art. 74 e considerando 79 EHDS.

transfrontaliero (ad es. le infrastrutture MyHealth@EU e HealthData@EU); dall'altro, stabilisce una base giuridica comune per i trattamenti di dati sanitari elettronici personali. Al tempo stesso, però, non può ignorarsi la presenza di disposizioni nello EHDS che potrebbero generare una situazione di frammentazione normativa tale da costituire un ostacolo per la libera circolazione dei dati sanitari personali e che richiederanno pertanto un'attenzione particolare da parte dei legislatori nazionali affinché non si ripetano i problemi emersi con l'applicazione del GDPR.

Sarà, ad esempio, necessario un coordinamento tra gli Stati membri – possibilmente favorito dall'attività del Comitato sullo EHDS [188] – per garantire un'applicazione uniforme dei diritti riconosciuti alle persone fisiche, soprattutto per quanto riguarda le limitazioni a tali diritti [189], rispetto alle quali gli Stati membri mantengono un certo margine di discrezionalità. Lo stesso discorso vale per la facoltà concessa al legislatore nazionale di: i) introdurre il diritto di *opt-out* all'uso primario e di stabilire, a questo proposito, regole o garanzie specifiche per alcune categorie di dati sanitari (ad es. i dati genetici) [190]; ii) adottare misure volte a consentire, in specifiche circostanze, l'accesso ai dati per uso secondario, rispetto ai quali è stato esercitato il diritto di *opt-out* [191]; iii) mantenere o introdurre ulteriori condizioni *ex* art. 9, par. 4, GDPR per il trattamento di dati genetici, provenienti da applicazioni per il benessere o biobanche, nonché dati molecolari [192].

Al di là di tali profili critici, le scelte compiute con lo EHDS, anche se perfettibili, testimoniano un diverso modo di bilanciare il diritto alla protezione dei dati personali e gli altri diritti e interessi in gioco, riconoscendo come l'uso e la condivisione dei dati sanitari, anche a livello transfrontaliero, possano contribuire alla salute delle persone fisiche e della collettività. Alla luce di tali sviluppi, appare quanto mai opportuno interrogarsi sulla coerenza tra gli obiettivi perseguiti dallo EHDS e quelli delineati nel GDPR, valutando la possibilità di rimuovere taluni ostacoli normativi alla libera circolazione dei dati personali, sia attraverso una revisione del testo del GDPR (sezione 3.1)

---

[188] Art. 94 EHDS.

[189] Oltre agli esempi menzionati nel testo, si vedano anche le restrizioni che il diritto nazionale può stabilire al diritto di condivisione selettiva dei dati (artt. 8 e 13, par. 4, EHDS) e al diritto a ricevere informazioni (art. 9 EHDS).

[190] Art. 10 e considerando 18 EHDS.

[191] Art. 71, parr. 4-6, e considerando 54 EHDS.

[192] Art. 51, par. 3, EHDS. Disposizione ritenuta problematica per la condivisione transfrontaliera dei dati anche da F. KERTESZ, *Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union*, in *EJHL*, 2024, vol. 31, n. 5, p. 509. L'autore sottolinea inoltre che la mancanza di coerenza nell'utilizzo delle tecniche di pseudonimizzazione e anonimizzazione può costituire un ulteriore ostacolo alla libera circolazione dei dati.

sia, nelle more, mediante interventi sulle normative nazionali di attuazione che si presentano maggiormente problematiche rispetto al perseguimento di tale obiettivo (sezione 3.2).

3.1. Alcune ipotesi di revisione del testo del GDPR

Il percorso che ha portato all'adozione del GDPR, iniziato nel 2012 [193], si è concluso in un contesto storico in cui molte delle sue disposizioni apparivano già inadeguate per affrontare le sfide poste dal processo di digitalizzazione, che stava progressivamente interessando un numero crescente di settori economici e sociali. Ciononostante, negli anni successivi all'entrata in vigore del GDPR, l'ipotesi di una sua revisione è stata raramente presa seriamente in considerazione. Tra le possibili ragioni di tale reticenza vi è il forte legame tra la disciplina europea per la protezione dei dati personali e il diritto fondamentale di cui all'art. 8 Carta, che rende complesso ipotizzare un intervento normativo senza il rischio di una regressione nella tutela delle prerogative degli interessati. Inoltre, il GDPR è visto come uno degli esperimenti normativi di maggior successo dell'Unione, rappresentando l'emblema del modello valoriale europeo nel mondo digitale, da esportare anche oltre i suoi confini.

Sebbene questi fattori non siano da sottovalutare, le potenzialità del GDPR per tutelare i diritti e gli interessi dei singoli e della collettività rischiano di rimanere inespresse qualora, unitamente a un cambiamento nella sua interpretazione, non si intraprenda un serio processo di revisione del GDPR volto a superare i numerosi profili critici connessi alla sua applicazione [194].

Un primo passo in questa direzione è stato compiuto dalla Commissione nel 2023 con una proposta di regolamento finalizzato ad armonizzare i (soli) aspetti procedurali del trattamento dei dati personali in casi transfrontalieri [195],

---

[193] Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), 2012/0011 (COD).

[194] A questo proposito, cfr. COM(2020) 264 final; documento di lavoro dei servizi della Commissione che accompagna la Comunicazione della Commissione al Parlamento europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, SWD(2020) 115 final, del 24 giugno 2020; Risoluzione del Parlamento europeo sulla relazione di valutazione della Commissione; Posizione e conclusioni del Consiglio in merito all'applicazione del GDPR.

[195] Proposta di regolamento che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679, COM/2023/348 final, del 4 luglio 2023 (proposta di regolamento sulle norme procedurali). Su di essa si sono espressi l'EDPB e l'EDPS con il parere congiunto n. 01/2023, e nel corso dell'iter legislativo il testo ha subìto modifiche

adottata ufficialmente a dicembre 2025 [196]. L'intervento mira, in particolare, a definire regole comuni in materia di reclami e diritti procedurali delle parti interessate – sia i soggetti sottoposti a indagine, sia i reclamanti – garantendo, ad esempio, il diritto di essere ascoltati e l'accesso ai fascicoli amministrativi. L'iniziativa intende inoltre promuovere un'armonizzazione giuridica sui criteri di ricevibilità o rigetto dei reclami, sui poteri istruttori delle autorità di controllo, sui termini procedurali e sull'attuazione operativa dei meccanismi di cooperazione e risoluzione delle controversie previsti rispettivamente dagli artt. 60 e 65 GDPR, con l'obiettivo di semplificarne e renderne più efficace il funzionamento.

A livello sostanziale manca ancora una proposta normativa analoga, benché la Commissione von der Leyen II abbia avviato un processo di modifica del GDPR nell'ambito del *Digital Omnibus* [197], presentato a metà novembre 2025 con l'obiettivo dichiarato di rafforzare la competitività dell'Unione – in linea con le raccomandazioni contenute nei Rapporti Letta e Draghi – e di favorire una più ampia disponibilità di dati, così da "sbloccarne" il potenziale ai fini dello sviluppo dell'IA [198].

---

rilevanti sia da parte del Parlamento europeo sia del Consiglio. Il Parlamento ha adottato la propria posizione negoziale in prima lettura il 10 aprile 2024, mentre il Consiglio ha definito il *general approach* il 13 giugno 2024. Per un commento critico della proposta, v. F. BRITO BASTOS, P. PALKA, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity*, in *ECLR*, 2023, n. 3, p. 495; L. MUSTERT, *The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?*, in *Eur. Data Prot. L. Rev.*, 2023, vol. 9, n. 4, pp. 454-464; E. FRONCZAK, *The Good, the Bad and the Ugly – A Take on the Commission Proposal for a GDPR Procedural Regulation*, in *Eu Law Live*, 2023; C.H. HOFMANN, L. MUSTERT, *Procedures Matter – What to Address in GDPR Reform and a New GDPR Procedural Regulation*, in *Eu Law Live*, 2023. Per quanto riguarda invece gli emendamenti presentati dal Parlamento, si rimanda all'analisi di E. FRONCZAK, *Light on the Horizon for Transnational GDPR Enforcement: The EP Breathes Life into the Proposed Procedural Regulation*, in *Eu Law Live*, 2024; EDPB, *Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR*.

[196] Regolamento (UE) 2025/2518 del Parlamento europeo e del Consiglio, del 26 novembre 2025, che stabilisce norme procedurali aggiuntive sull'applicazione del regolamento (UE) 2016/679. Per una prima analisi critica del regolamento, cfr. MUSTERT L., *Proceduralising GDPR Enforcement: How Complexity May Undermine Effective Cross-Border Data Protection*, in *Eur. Data Prot. L. Rev.*, 2025, vol. 11, n. 4, pp. 498-510.

[197] Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 e delle 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 della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025.

[198] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Data Union Strategy. Unlocking Data for AI*, COM(2025) 835 final.

Accanto alle (inaspettate) modifiche a definizioni chiave come "dato personale" e "ricerca scientifica" – mirate, da un lato, a valorizzare i recenti orientamenti della Corte per circoscrivere l'ambito di applicazione materiale del GDPR [199] e, dall'altro, ad agevolare le attività di ricerca anche quando perseguono finalità commerciali [200] – le misure attualmente prospettate si concentrano soprattutto sulla riduzione degli oneri normativi a carico delle imprese, in particolare quelli informativi [201], e sull'ampliamento delle possibilità di trattare dati personali, anche appartenenti a categorie particolari, per lo sviluppo di sistemi di IA [202], più che su una riforma complessiva del regolamento.

Emblematico, in tal senso, è il mancato intervento sulle c.d. clausole facoltative di specificazione, il cui impiego diffuso da parte degli Stati membri è stato più volte indicato come una delle principali cause di frammentazione normativa, in contrasto con l'obiettivo del GDPR di garantire la libera circolazione dei dati personali all'interno dell'Unione [203].

A questo proposito, le istituzioni europee si sono finora limitate a promuovere un maggiore coordinamento tra gli Stati membri, suggerendo l'adozione

---

[199] Art. 3, par. 1, lett. a), *Digital Omnibus*.

[200] Art. 3, par. 1, lett. b), n. 35, *Digital Omnibus*.

[201] Art. 3, parr. 4-6, *Digital Omnibus*. In modo analogo, l'*Omnibus package* presentato a maggio 2025 si concentra sull'obiettivo di alleggerire il carico regolatorio per le imprese. Come si evince dai considerando 8-11 e dall'art. 1 della proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2016/1036, (UE) 2016/1037, (UE) 2017/1129, (UE) 2023/1542 e (UE) 2024/573 per quanto riguarda l'estensione di alcune misure attenuanti disponibili per le piccole e medie imprese alle piccole imprese a media capitalizzazione e ulteriori misure di semplificazione, COM(2025)501 final, del 21 maggio 2025, le principali novità riguardano l'ampliamento della deroga all'obbligo, per il titolare del trattamento, di tenere un registro delle attività di trattamento (art. 30, par. 5, GDPR). Tale deroga verrebbe estesa alle imprese o organizzazioni con meno di 750 dipendenti (anziché 250, come previsto attualmente), a condizione che il trattamento non presenti un rischio elevato per i diritti e le libertà degli interessati, in conformità con quanto previsto dall'art. 35 GDPR. Ulteriori modifiche interessano le disposizioni relative ai codici di condotta (art. 40 GDPR) e ai meccanismi di certificazione, sigilli e marchi di protezione (art. 42 GDPR), che dovrebbero essere adattati per tenere adeguatamente conto delle esigenze e degli interessi delle piccole e medie imprese. In linea generale, la proposta della Commissione è stata accolta con favore da EDPB e EDPS nel parere congiunto n. 01/2025 sulla proposta di regolamento relativo alle misure di semplificazione per le PMI e le SMC, in particolare per quanto riguarda l'obbligo di conservazione dei dati ai sensi dell'articolo 30, par. 5, GDPR. Non sono tuttavia mancate osservazioni e richieste di chiarimento, volte a garantire che le semplificazioni proposte non compromettano il livello di tutela dei diritti degli interessati.

[202] Art. 3, par. 3, lett. a) e par. 15, *Digital Omnibus*.

[203] COM(2020) 264 final, p. 8; Risoluzione del Parlamento europeo sulla relazione di valutazione della Commissione, p. 6; Posizione e conclusioni del Consiglio in merito all'applicazione del GDPR, p. 11.

di orientamenti supplementari da parte dell'EDPB o di codici di condotta *ex* art. 40 GDPR. Per quanto riguarda le norme che regolano i trattamenti ai fini di ricerca scientifica, ad esempio, la Commissione ha invitato – per ora senza successo – l'EDPB a pubblicare linee guida chiarificatrici e a riesaminare, alla luce degli sviluppi tecnologici, quelle adottate in precedenza [204]. Allo stesso modo, il Parlamento europeo e il Consiglio hanno sottolineato l'esigenza che l'EDPB si esprima sul significato di disposizioni centrali in questo settore, come il considerando 50 GDPR sulla presunzione di non incompatibilità per i trattamenti di dati a fini di ricerca scientifica [205].

Benché tali sollecitazioni non siano state ancora colte, l'azione dell'EDPB potrebbe rivelarsi cruciale per avviare (o meglio, accompagnare) un futuro processo di modifica [206], così come è avvenuto per gli aspetti procedurali del GDPR. È stato infatti grazie all'adozione della dichiarazione di Vienna [207] e alla successiva lettera inviata alla Commissione [208] che quest'ultima ha lanciato un'iniziativa per specificare le regole del GDPR sull'*enforcement* [209].

---

[204] COM(2020) 264 final, pp. 8-9. Nel 2021, il DG SANTE ha indicato, tra i potenziali interventi sovranazionali futuri, la predisposizione di un codice di condotta, eventualmente con validità generale *ex* art. 40, par. 9, GDPR, per fornire indicazioni sull'interpretazione di concetti chiave del GDPR, come gli standard tecnici per l'anonimizzazione e pseudonimizzazione dei dati sanitari, la natura e la forma del consenso come condizione di liceità e garanzia, e la ripartizione delle responsabilità nelle ipotesi di contitolarietà *ex* art. 26 GDPR (DG SANTE, *op. cit*., 2021, pp. 130-135).

[205] Risoluzione del Parlamento sulla relazione di valutazione della Commissione, p. 4 e su rafforzare l'Europa nella lotta contro il cancro – Verso una strategia globale e coordinata (2020/2267(INI)), par. 179; Posizione e conclusione del Consiglio in merito all'applicazione del GDPR, p. 6. Anche l'Agenzia dell'Unione europea per i diritti fondamentali ha sollecitato l'EDPB a chiarire i dubbi circa l'interpretazione da fornire all'art. 89 GDPR in modo da supportare le autorità di controllo nazionali nello svolgimento dei loro compiti consultivi nei confronti dei ricercatori che intendono utilizzare dati personali (cfr. *GDPR in Practice, Experiences of Data Protection Authorities*, 2024).

[206] Tuttavia, a tale proposito, non può non ignorarsi la valutazione positiva sulla tenuta del GDPR da parte dell'EDPB: *Contribution of the EDPB to the Report on the Application of the GDPR under Article 97*, 2023.

[207] In questa dichiarazione, l'EDPB ha individuato "*a list of procedural aspects that could be further harmonised in EU law to maximise the positive impact of GDPR cooperation*". Cfr. EDPB, *Statement on enforcement cooperation*, 2022: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-enforcement-cooperationen.

[208] Nell'allegato di questa lettera vi è "*a list of procedural aspects that could benefit from further harmonisation at EU level, with a view of making sure that national procedures do not hinder the full effectiveness of the GDPR's cooperation and consistency mechanism*". Cfr. *Letter to the EU Commission on Procedural Aspects that Could be Harmonised at EU Level*, 2022: https://edpb.europa.eu/system/files/2022-10/edpbletterout2022-0069totheeucommissiononproceduralaspectsen0.pdf.

[209] *Commission initiative to further specify procedural rules relating to the enforcement of the*

Nel frattempo, un ruolo cruciale può essere svolto dal mondo accademico nel pungolare il processo legislativo, suggerendo strategie per superare le debolezze del GDPR, non solo riguardo ai limiti delle norme procedurali dello stesso, ma anche rispetto alla situazione di frammentazione normativa creatasi a seguito della diversa applicazione da parte degli Stati membri delle clausole di specificazione facoltative.

Con particolare riferimento all'uso dei dati sanitari per finalità di ricerca scientifica, tra le proposte che ricorrono più frequentemente vi sono quelle che insistono sulla necessità di spostare l'attenzione dal consenso alla trasparenza e al diritto degli interessati a essere informati [210]. Al contempo, si propone di fare maggiore affidamento, nella valutazione della legittimità delle attività di trattamento, ai comitati etici competenti, piuttosto che alle autorità di controllo [211]. Inoltre, per superare la frammentazione normativa derivante dall'interpretazione disomogenea del GDPR, alcuni autori auspicano un ricorso più sistematico al meccanismo di coerenza [212] a un'armonizzazione *bottom-up* attraverso la creazione di codici di condotta settoriali *ex* art. 40 GDPR [213].

Nel solco di tale dibattito dottrinale, si intende qui avanzare alcune proposte di revisione delle disposizioni del GDPR sui trattamenti di dati sanitari per finalità di ricerca scientifica. Nello specifico, una volta delimitato l'ambito applicativo della disciplina, precisando il significato da attribuire alla finalità di "ricerca scientifica" (sezione 3.1.1), ci concentreremo sulle disposizioni che regolano queste ipotesi di trattamento [214]. L'obiettivo è formulare proposte di

---

General Data Protection Regulation (GDPR): https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulationen.

[210] R. DUCATO, *op. cit*., 2020.

[211] S. SLOKENBERGA, O. TZORTZTATOU, J. REICHEL (eds.), *op. cit*., 2021.

[212] M.L. MANIS, *The Processing of Personal Data in the Context of Scientific Research. The New Regime under the EU-GDPR*, in *BioLaw Journal*, 2017, n. 3, pp. 325-354.

[213] Cfr. EDPS, *Preliminary Opinion on Scientific Research*, 2020, p. 25. In dottrina, si rinvia a W. BIRGIT et al., *Putting the GDPR into Practice: Difficulties and Uncertainties Experienced in the Conduct of Big Data Health Research*, in *Eur. Data Prot. L. Rev*., 2021, vol. 7, p. 206; F. MOLNÁR-GÁBOR, *op. cit*., 2022, p. 281; D. TOWNEND, *Conclusion: Harmonization in Genomic and Health Data Sharing for Research: an Impossible Dream?*, in *Human Genetics*, 2018, vol. 137, pp. 657-664; J. REICHEL, *Allocation of Regulatory Responsibilities: Who Will Balance Individual Rights, the Public Interest and Biobank Research Under The GDPR?*, in S. SLOKENBERGA, O. TZORTZTATOU, J. REICHEL (eds.), *op. cit.*, 2021, p. 430; B. WOUTERS et al., *op. cit.*, 2021, p. 215; M. PHILIPPS, B.M. KNOPPERS, *Whose Commons? Data Protection as a Legal Limit of Open Science*, in *J. Law Med. Ethics*, 2019, vol. 47, pp. 109-110.

[214] Più precisamente, il focus sarà sugli artt. 9, par. 2, lett. j), 9, par. 4, e 89 GDPR. Al contrario, non verrà preso in considerazione l'art. 9, par. 2, lett. i), GDPR (trattamenti per motivi di interesse pubblico per motivi di sanità pubblica) che, pur potendo rappresentare una base giuridica valida anche per trattamenti di dati relativi alla salute ai fini di ricerca scien-

modifica che consentano di fissare una soglia minima di bilanciamento *ex lege*, volta a sistematizzare i diritti e gli interessi in gioco, da integrare successivamente con una ponderazione da compiere *ex post* (sezione 3.1.2). I cambiamenti ipotizzati sono pensati per rendere la disciplina del GDPR, nel rispetto dei limiti costituzionali posti dall'ordinamento europeo, maggiormente coerente agli obiettivi perseguiti dal GDPR, oltre che, in ambito sanitario, dallo EHDS.

3.1.1. Una definizione comune di "ricerca scientifica"

Nel testo del GDPR manca una definizione univoca e puntuale di "ricerca scientifica". Il legislatore europeo ha infatti optato per una formulazione volutamente ampia, ricomprendendovi, a titolo esemplificativo, le attività di sviluppo tecnologico e quelle di ricerca applicata, anche quando promosse e finanziate da soggetti privati [215]. Tale scelta, pur funzionale agli obiettivi di costruzione di uno spazio europeo della ricerca ai sensi dell'art. 179 TFUE e di promozione dell'innovazione [216], è stata oggetto di rilievi critici, in quanto

---

tifica, è stato formulato in modo da non lasciare agli Stati membri un margine di manovra particolarmente ampio: non è richiesto di verificare il rispetto dell'"essenza del diritto alla protezione dei dati personali" e la proporzionalità del trattamento rispetto alle finalità perseguite. Inoltre, senza rinviare alle salvaguardie e alle deroghe di cui all'art. 89 GDPR, viene solamente specificato che il diritto dell'Unione o degli Stati membri sulla base del quale tale trattamento viene effettuato deve prevedere "misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale". Sulle differenze tra le condizioni di liceità previste dall'art. 9 GDPR, cfr. G. COMANDÉ, G. SCHNEIDER, *op. cit.*, 2022(a), p. 570 ss.

[215] Secondo il considerando 159 GDPR, "[n]ell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica". Tra coloro che ritengono che all'interno della definizione di ricerca contenuta nel GDPR debba essere compresa anche quella privata, cfr. P. AURUCCI, *op. cit*., 2023, p. 140; O. TENE, J. POLONETSKY, *Beyond IRBs: Ethical Guidelines of Data Research*, in *Wash. Lee Law Rev.*, 2016, vol. 72, p. 458 ss.; S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Interferences: Re-thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Bus. Law Rev.*, 2019, vol. 2, p. 495 ss. Per una sistematizzazione delle diverse nozioni di "ricerca scientifica" nel vigente quadro normativo europeo, cfr. L. PASERI, *Defining Scientific Research Within the EU's Politics of Data: The Impact on Personalized Smart Medicine*, in F. CASAROSA, F. GENNARI, A. ROSSI (eds), *Enabling and Safeguarding Personalized Medicine*, Springer, Cham, 2025, p. 17 ss.

[216] Considerando 53, 157 e 159 GDPR. L'EDPS ha evidenziato come il regime di maggiore flessibilità concesso ai trattamenti per finalità di ricerca scientifica "*is afforded on the assumption that research occurring within a framework of ethical oversight serves, in principle, the public interest*" e "*the role of research is understood to provide knowledge that can, in turn,*

sembra presupporre che la ricerca scientifica sia, in quanto tale, intrinsecamente meritevole di tutela e di deroghe al regime ordinario di protezione dei dati, indipendentemente dalle finalità concrete perseguite.

Questa impostazione è messa in discussione da casi emblematici in cui il richiamo alla "ricerca scientifica" ha finito per mascherare finalità prevalentemente economiche o manipolative, difficilmente riconducibili al pubblico interesse. Si pensi, da un lato, al caso Cambridge Analytica, nel quale i dati personali sono stati utilizzati per influenzare indebitamente il consenso elettorale; dall'altro, all'esperienza della società 23andMe, che ha ceduto dati genetici, originariamente raccolti sulla base del consenso degli interessati, a imprese farmaceutiche quali Pfizer e Janssen [217]. In entrambi i casi, il richiamo alla "ricerca scientifica" ha mascherato finalità economiche e operative ben distanti dal pubblico interesse.

Per evitare simili derive, senza privarsi dell'enorme quantità di dati in mano ai soggetti privati [218] e delle loro capacità di innovare [219], prevedendo che possano beneficiare delle deroghe previste dal GDPR esclusivamente quei progetti che, indipendentemente dalla natura pubblica o privata dei soggetti promotori, perseguano obiettivi effettivi di ampliamento della conoscenza e di promozione del benessere collettivo [220]. Un simile approccio risulterebbe

---

improve the quality of life for a number of people and improve the efficiency of social services" (EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 2020, p. 11).

[217] H.B. BENTZEN, *In the Name of Scientific Advancement: How to Assess What Constitutes 'Scientific Research' in the GDPR to Protect Data Subjects and Democracy*, in G. TERZIS et al. (eds.), *Disinformation and Digital Media as a Challenge for Democracy*, Intersentia, Cambridge, 2020, pp. 342-343.

[218] Il ruolo dei soggetti privati è emerso con particolare evidenza durante la pandemia, quando si è constatato come tali attori, accanto alle autorità pubbliche, possano contribuire in modo concreto al perseguimento dell'interesse pubblico (linee guida dell'EDPB n. 03/2020 sul trattamento dei dati relativi alla salute ai fini di ricerca scientifica nel contesto dell'emergenza legata al Covid-19, 2020, punto 64). In questa prospettiva può essere letto anche l'obbligo, previsto dal DA, per i soggetti privati di mettere a disposizione i dati sulla base di necessità eccezionali, come un'emergenza sanitaria (art. 14 DA).

[219] Risoluzione del Parlamento europeo dell'8 luglio 2021 su un nuovo spazio europeo della ricerca e dell'innovazione (2021/2524(RSP)), punto 24.

[220] Un'interpretazione simile della nozione di ricerca scientifica è stata suggerita dall'EDPS nella *Preliminary Opinion on Data Protection and Scientific Research*, 2020, p. 12. In senso analogo, in dottrina, cfr. E-B. VAN VEEN, *op. cit.*, 2018, p. 76; J. MESZAROS, C-H. HO, *AI Research and Data Protection: Can the Same Rules Apply for Commercial and Academic Research under the GDPR?*, in *Comput. Law Secur. Rev.*, 2021, vol. 41, p. 9. All'opposto, S. SLOKENBERGA, *op. cit.*, 2021, pp. 21-22 sottolinea che la linea interpretativa elaborata dall'EDPS, oltre a non considerare la complessità della realtà in cui le attività di ricerca vengono svolte, non è rispettosa della scelta del legislatore di intendere in senso ampio la nozione di ricerca scientifica. Lo stesso viene argomentato da L. MARELLI, G. TESTA, I. VAN HOYWEGHEN, *Big Tech Platforms in Health Research: Re-Purposing Big Data Governance in*

coerente con gli orientamenti interpretativi espressi dall'EDPB [221] e dall'EDPS [222], nonché con le più recenti prese di posizione della Commissione [223], che sottolineano come la ricerca scientifica non possa essere disgiunta da esigenze di responsabilità, trasparenza e fiducia.

Questa esigenza di riallineamento emerge con particolare chiarezza nel confronto con lo EHDS. Anche tale strumento adotta una concezione ampia della finalità di ricerca scientifica [224] e valorizza in modo significativo l'uso secondario dei dati sanitari da parte di soggetti pubblici, privati e non profit. Tuttavia, a differenza del GDPR, lo EHDS subordina espressamente l'accesso e l'uso dei dati sanitari a progetti che contribuiscano alla salute pubblica, alla valutazione delle tecnologie sanitarie o al miglioramento della qualità, sicurezza ed efficacia delle cure, dei farmaci e dei dispositivi medici [225]. L'obiettivo dichiarato è garantire un beneficio concreto e verificabile per i pazienti, gli operatori sanitari e i decisori pubblici.

Di conseguenza, tra le finalità di ricerca scientifica idonee a giustificare l'uso secondario dei dati ai sensi dell'art. 53 EHDS rientrano sia le attività di sviluppo e innovazione – come la progettazione di nuovi farmaci, dispositivi medici, prodotti e servizi sanitari accessibili ed economicamente sostenibili per i cittadini dell'Unione – sia quelle volte a migliorare la disponibilità e l'equità di accesso a tali risorse in tutti gli Stati membri. Rientrano altresì in tale ambito l'addestramento, la valutazione e lo sviluppo di algoritmi destinati all'impiego nell'assistenza sanitaria e nella cura delle persone fisiche, tra cui dispositivi medici, sistemi di intelligenza artificiale e applicazioni di sanità digitale [226]. In tal modo, lo EHDS offre un possibile modello per una nozione finalisticamente orientata

---

Light of the General Data Protection Regulation's Research Exemption, in *Big Data & Society*, 2021, vol. 8, pp. 5-6.

[221] Linee guida dell'EDPB n. 05/2020, 2020, par. 153.

[222] EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 2020, p. 12 e *Study on the Secondary Use of Personal Data in the Context of Scientific Research*, Final Report EDPS/2019/02-04, p. 16 ss.

[223] Tra le modifiche al GDPR contenute nel *Digital Omnibus*, infatti, la Commissione ha proposto una nozione ampia di ricerca scientifica comprensiva anche di attività a sostegno dell'innovazione con finalità commerciali, purché volte alla crescita della conoscenza e rispettose degli standard etici del settore (art. 3, par. 1, lett. b), n. 35, *Digital Omnibus*).

[224] Secondo il considerando 61 EHDS, la nozione di "finalità di ricerca scientifica" deve essere interpretata in senso ampio, comprendendo, ad esempio, lo sviluppo tecnologico e la sperimentazione, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata da privati.

[225] Art. 53, par. 1, lett. e), EHDS.

[226] Rimane, invece, fuori dalla nozione di ricerca scientifica presente nello EHDS, l'erogazione di assistenza sanitaria personalizzata che consiste nel valutare, mantenere o ripristinare lo stato di salute delle persone fisiche sulla base dei dati sanitari di altre persone fisiche (art. 53, par. 1, lett. f), EHDS).

della nozione di ricerca scientifica, idonea a limitare derive opportunistiche senza sacrificare il potenziale innovativo dei dati.

3.1.2. Le misure di garanzia e il margine di manovra degli Stati membri

Unitamente alla definizione del concetto di "ricerca scientifica", sarebbe opportuno chiarire i contorni delle "garanzie adeguate per i diritti e le libertà dell'interessato" che l'art. 89 GDPR richiede per trattare dati personali ai fini di ricerca scientifica. La scelta di lasciare al titolare del trattamento il compito di individuare tali garanzie, anche se rispettosa dell'approccio basato sul rischio [227] e del principio di *accountability* [228], risulta problematica rispetto alla realizzazione dell'obiettivo di libera circolazione dei dati personali. Potrebbe infatti succedere che, anche a seconda delle valutazioni compiute da DPO o autorità di controllo, le garanzie adottate dai titolari varino sensibilmente da uno Stato membro all'altro, con potenziali effetti dissuasivi o pratiche opportunistiche rispetto alla decisione di avviare progetti di ricerca transazionali.

Per favorire una maggiore armonizzazione, si potrebbe prevedere l'inserimento, direttamente nel testo vincolante del GDPR [229], di un elenco esaustivo di garanzie da considerarsi adeguate ai sensi dell'art. 89 GDPR, tenendo conto che tali misure sono essenziali per evitare lacune nella tutela degli interessati, connesse all'applicazione delle eccezioni ad alcuni diritti [230] e principi cardine

---

[227] Approccio di cui l'art. 35 del GDPR sulla valutazione d'impatto sulla protezione dei dati rappresenta l'emblema. Sul modello "*risk-based*" adottato con il GDPR, v. R. GELLERT, *Understanding the Notion of Risk in the General Data Protection Regulation*, in *Comput. Law Secur. Rev.*, 2018, vol. 34, p. 279; R. GELLERT, *We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection*, in *Eur. Data Prot. Law Rev*., 2016, vol. 2, p. 481; R. GELLERT, *Understanding Data Protection as Risk Regulation*, in *J. Internet Law*, 2015, vol. 18, p. 3; C. QUELLE, *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-Based Approach*, in *Eur. J. Risk Reg.*, 2018, vol. 9, p. 502; N. VAN DIJK, R. GELLERT, K. ROMMETVEIT, *A Risk to a Right? Beyond Data Protection Risk Assessments*, in *Comput. Law Secur. Rev.*, 2016, vol. 32, p. 286.

[228] Art. 5, par. 2, GDPR.

[229] Ad oggi, per i trattamenti di dati effettuati per scopi di ricerca scientifica, gli unici esempi di garanzie adeguate per i diritti e le libertà dell'interessato sono forniti dal considerando 156 GDPR che riconduce in questa categoria le misure tecniche e organizzative finalizzate a garantire il principio di limitazione dei dati.

[230] Tra quelle previste dal GDPR, le deroghe al diritto dell'interessato a essere informato quando la comunicazione delle informazioni risulti impossibile o implichi uno sforzo sproporzionato, oppure quando tale comunicazione rischi di compromettere o pregiudicare gravemente il raggiungimento delle finalità del trattamento (art. 14, par. 5, lett. b), GDPR). Cfr. Linee guida del WP sulla trasparenza, WP 260 rev.01, 2018, punto 64 e EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, p. 21. Si vedano, inoltre, le deroghe

della disciplina (ad es. i principi di conservazione dei dati e limitazione delle finalità) [231]. In alternativa, tale elenco potrebbe essere incluso in un atto di esecuzione della Commissione – adottato secondo la procedura d'esame e soggetto quindi al controllo degli Stati membri –, nel quale, oltre a individuare in via generale le misure di garanzia ritenute adeguate, potrebbero essere forniti esempi specifici per ambiti settoriali, come quello sanitario [232].

Con riferimento alle misure generali, ispirandosi alle garanzie che sono previste con maggiore frequenza a livello nazionale, l'elenco potrebbe comprendere: i) anonimizzazione e pseudonimizzazione; ii) misure tecniche (ad es. accesso selettivo e crittografia) e organizzative (ad es. obblighi di confidenzialità e corsi di formazione specifici per il personale) [233]; iii) misure di sicurezza (ad es. cifratura, accordi di non divulgazione, registrazioni degli accessi ai dati); iv) codici di condotta. Per quanto concerne il settore sanitario, in linea con quanto previsto dallo EHDS per l'uso secondario dei dati sanitari elettronici, potrebbero essere considerate adeguate anche misure quali: i) il rispetto del divieto di re-identificazione [234]; ii) l'utilizzo dei dati all'interno di un ambiente sicuro di trattamento [235]; iii) la previsione di obblighi informativi che consentano di assicurare un livello sufficiente di trasparenza quanto alle modalità di utilizzo dei dati e i risultati raggiunti grazie al loro trattamento [236];

---

previste in relazione al diritto alla cancellazione (art. 17, par. 3, lett. d), GDPR) e al diritto di opposizione (art. 21, par. 6, GDPR). Diversamente, le deroghe che possono essere introdotte dagli Stati membri o dal diritto dell'Unione riguardano i diritti di accesso (art. 15), rettifica (art. 16), limitazione del trattamento (art. 18) e opposizione (art. 21). Per quanto riguarda i trattamenti effettuati a fini di ricerca scientifica – a differenza di quelli svolti per finalità di archiviazione nel pubblico interesse – non sono invece consentite deroghe al diritto alla notifica in caso di rettifica, cancellazione dei dati personali o limitazione del trattamento (art. 19), né all'esercizio del diritto alla portabilità (art. 20).

[231] In particolare, viene posto l'accento sui principi di minimizzazione e conservazione limitata, sui principi di integrità e riservatezza, nonché sul principio della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita (considerando 156 GDPR).

[232] Un approccio simile è stato individuato anche dall'EDPS in *Legal Study on the Appropriate Safeguards under Article 89(1) GDPR for the Processing of Personal Data for Scientific Research*, 2019, pp. 64-69.

[233] A tale proposito, rileva quanto disposto dall'art. 32, par. 1, lett. a) e b), GDPR che, concretizzando i principi di integrità e riservatezza di cui all'art. 5, par. 1, lett. f), GDPR, impone a qualsiasi titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza commisurato al rischio. Tali misure includono, in particolare, la pseudonimizzazione e la cifratura dei dati, nonché la capacità di assicurare, su base permanente, la riservatezza e l'integrità dei sistemi e dei servizi di trattamento.

[234] Art. 61, par. 3, EHDS.

[235] Art. 73 EHDS.

[236] Si vedano, ad esempio, gli obblighi di trasparenza che lo EHDS prevede per gli organismi responsabili dell'accesso ai dati sanitari (art. 58 e considerando 66 EHDS).

iv) l'attribuzione di compiti specifici per i comitati etici; v) la designazione del DPO; vi) lo svolgimento di una DPIA [237]

Nel testo normativo andrebbe inoltre chiarito che le garanzie previste non devono tradursi in un ostacolo alla libera circolazione dei dati personali all'interno dell'Unione [238] e dovrebbero essere adottate tenendo conto, da un lato, i rischi che una determinata attività di trattamento comporta per i diritti degli interessati e, dall'altro, i benefici che tale trattamento può generare per le persone fisiche e per la collettività nel suo complesso. In tal modo, qualora sia dimostrabile il perseguimento di un interesse pubblico, i titolari del trattamento potranno avvalersi con maggiore facilità delle deroghe previste, introducendo garanzie supplementari meno onerose. Al contrario, "*in case of for-profit research activities data subjects are entitled to a greater control over occurring processing operations due to a fuller application of data protection principles and rights and a more severe layer of safeguards that controllers need to enact*" [239].

Modifiche di questo tipo al testo del GDPR appaiono decisive anche per consentire l'operatività della presunzione di non incompatibilità che – è forse superfluo ricordare – non è assoluta ma subordinata alle condizioni di cui all'art. 89, par. 1, GDPR [240]. In tale prospettiva, e alla luce dei più recenti

---

[237] In dottrina, Kogut-Czarkowska e Shabani hanno individuato le reti federate (*federated networks*) come una misura di garanzia potenzialmente adeguata per facilitare la condivisione su larga scala dei dati sanitari a fini di ricerca biomedica, nel rispetto dei requisiti previsti dal GDPR e dallo EHDS. Tali reti, evitando la centralizzazione dei dati, risultano conformi ai principi di minimizzazione e riservatezza. Gli A. evidenziano, tuttavia, che persistono criticità, in particolare la necessità di chiarire le responsabilità dei soggetti partecipanti ai sensi del GDPR, nonché di sviluppare un quadro di governance solido. Cfr. M. KOGUT-CZARKOWSKA, M. SHABANI, *Federated Networks and Secondary Uses of Health Data – Challenges in Ensuring Appropriate Safeguards for Sharing Health Data Under the GDPR and EHDS*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Routledge, London, 2025, pp. 229-254.

[238] Tale specificazione è prevista al considerando 53 GDPR con riferimento alle ulteriori condizioni, incluse limitazioni, che gli Stati membri possono inserire *ex* art. 9, par. 4, GDPR con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

[239] Cfr. G. COMANDÉ, G. SCHNEIDER, *op. cit*., 2022(a), pp. 596. Una disposizione del GDPR che avvalora la tesi secondo la quale i titolari che svolgono trattamenti di dati per finalità di ricerca scientifica nell'interesse pubblico possono beneficiare di un regime meno rigoroso è l'art. 21, par. 6, che prevede una deroga al diritto di opposizione dell'interessato qualora il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

[240] Art. 5, par. 1, lett. b) e considerando 50 GDPR. Secondo queste disposizioni, il trattamento ulteriore per scopi di ricerca scientifica dovrebbe essere considerato lecito e compatibile qualora il trattamento originario sia tale sulla base del "contesto in cui i dati personali sono stati raccolti", delle "ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo", "della natura dei dati personali", "delle conseguenze dell'ulteriore trattamento previsto per gli interessati", e "del-

sviluppi in materia di uso secondario previsti dallo EHDS, appare opportuno abbandonare l'interpretazione restrittiva proposta dall'EDPS, secondo cui anche il riutilizzo dei dati per finalità di ricerca sarebbe soggetto all'obbligo di effettuare il test di compatibilità di cui all'art. 6, par. 4, GDPR [241]. Questa interpretazione impone infatti una valutazione caso per caso che consideri elementi come il nesso tra finalità originaria e secondaria, il contesto della raccolta, la natura dei dati trattati e le ragionevoli aspettative degli interessati [242], con il rischio di svuotare di efficacia la presunzione stessa e ostacolare attività di ricerca potenzialmente di rilevante interesse pubblico.

Una volta chiarita la portata delle garanzie di cui all'art. 89 GDPR, occorrerebbe definire in modo più preciso il rapporto tra queste e le "misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" prescritte dall'art. 9, par. 2, lett. j), GDPR, nonché le "ulteriori condizioni, comprese limitazioni" che gli Stati membri possono mantenere o

---

l'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto" (parere del WP n. 03/2013). Se, secondo il WP29, una base giuridica deve comunque esistere anche quando opera la deroga al principio di limitazione delle finalità (*Ibid.* p. 33), la dottrina non è giunta a conclusioni univoche. Una prima posizione, valorizzando quanto affermato nel considerando 50, ritiene che il trattamento ulteriore per finalità compatibili non richieda una nuova base giuridica rispetto a quella originaria. Una seconda impostazione sostiene invece la necessità che l'ulteriore trattamento sia fondato su una delle basi giuridiche di cui all'art. 6, par. 1, GDPR, poiché una deroga al principio di liceità non potrebbe derivare da un considerando. Secondo un'ulteriore interpretazione, infine, la base giuridica per il trattamento ulteriore dovrebbe coincidere con quella del trattamento iniziale. H.B. BENTZEN, *op. cit*., 2020, p. 402 sintetizza efficacemente tali diverse linee argomentative. Si vedano inoltre: A. PARZIALE, E. PULICE, D. MASCALZONI, *Mass-Scale G2B Data Sharing in an Emergency: between the GDPR, Data Governance Act, and European Health Data Space*, in *European Journal of Health Law*, 2025, p. 15; R. BECKER et al., *op. cit.*, 2023, pp. 137-138; S. AIDINLIS, *Government-to-Business (G2B) Research Data Sharing and the GDPR: Reconciling the 'Public' with the 'Private'?*, in E. KOSTA, R. LEENES, I. KAMARA, (eds.), *Research Handbook on EU Data Protection Law*, Edward Elgar, Cheltenham, 2022, p. 131.

[241] In questa direzione si inserisce la proposta della Commissione di modificare l'art. 5, par. 1, lett. b), GDPR, eliminando la necessità della valutazione caso per caso prevista dall'art. 6, par. 4, GDPR, qualora siano rispettate le garanzie di cui all'art. 89, par. 1, GDPR (art. 3, par. 2, proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 e delle 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 della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025).

[242] EDPS, *Preliminary Opinion on Data Protection and Scientific Research*, 2020, p. 23, in cui si stabilisce che il considerando 50 GDPR non esclude la necessità di applicare il test di cui all'art. 6, par. 4, GDPR, in quanto non è possibile sovrapporre il piano della legittimità con quello della specificazione delle finalità. A questo proposito, ulteriori delucidazioni dovrebbero arrivare dall'EDPB, come annunciato nel documento in risposta alla domanda di chiarimenti della Commissione europea e nelle linee guida n. 03/2020.

introdurre ai sensi dell'art. 9, par. 4, GDPR con riguardo al trattamento di dati genetici, biometrici o relativi alla salute. Attualmente, le due previsioni si collocano su piani distinti: le garanzie di cui all'art. 89 GDPR sono rimesse all'autonoma determinazione del titolare del trattamento, mentre le misure di cui all'art. 9, par. 2, lett. j), GDPR richiedono un fondamento legislativo nazionale o unionale. Tuttavia, proprio questa distinzione può generare incertezza, frammentazione e ostacoli alla circolazione dei dati tra Stati membri, specie nel contesto della ricerca transnazionale.

Sarebbe pertanto auspicabile un intervento normativo che promuova un maggiore coordinamento tra le due disposizioni, chiarendo che l'elenco delle garanzie considerate adeguate ai sensi dell'art. 89 GDPR possa, ove formalizzato a livello europeo, valere anche come parametro per le "misure appropriate e specifiche" richieste ai fini della liceità del trattamento dei dati sensibili *ex* art. 9, par. 2, lett. j), GDPR. In tal modo, si ridurrebbe il margine di discrezionalità lasciato ai titolari, garantendo maggiore certezza del diritto e una più uniforme tutela degli interessati nell'ambito delle attività di ricerca scientifica.

Con riferimento poi al quarto paragrafo dell'art. 9 GDPR, è stato già evidenziato come questa disposizione possa essere causa di frammentazione normativa all'interno dell'Unione e rappresentare un adempimento particolarmente oneroso per il titolare del trattamento, specialmente se combinata con l'art. 89 GDPR. Per questo motivo, l'art. 9, par. 4, GDPR dovrebbe essere modificato specificando che: i) le "ulteriori condizioni" introdotte a livello nazionale non devono ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero [243]; ii) le conseguenze pratiche derivanti da queste condizioni non devono rappresentare un adempimento eccessivo per i titolari del trattamento [244].

Inoltre, sarebbe opportuno inserire un inciso in cui, come per i trattamenti per finalità giornalistiche [245], viene previsto un obbligo di notifica alla Commissione delle "ulteriori condizioni". In questo modo, una volta valutata la

---

[243] Attualmente, questa specifica viene fatta solo all'interno del considerando 53 GDPR che, non occorre ricordare, è privo di vincolatività.

[244] Tale modifica andrebbe a codificare quanto espresso dalla Corte nella sentenza del 21 dicembre 2023, causa C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:1022. In questa occasione, i giudici hanno sottolineato che, qualora gli Stati decidano di avvalersi del margine discrezionale concesso loro dall'art. 9, par. 4, GDPR, questi dovrebbero, in linea con il principio di proporzionalità, "garantire che le conseguenze pratiche, segnatamente di ordine organizzativo, economico e sanitario, derivanti dagli ulteriori obblighi […] non siano eccessive nei confronti dei titolari di un tale trattamento, i quali non dispongono necessariamente di dimensioni o di risorse tecniche e umane sufficienti per soddisfare tali obblighi. Infatti, queste ultime non possono pregiudicare l'effetto utile dell'autorizzazione al trattamento che è espressamente prevista dall'art. 9, paragrafo 2, lettera h)" (punto 67).

[245] Art. 85, par. 3, GDPR.

stretta necessità delle misure nazionali e la loro conformità ai principi del GDPR, la Commissione potrebbe decidere di ricorrere alla Corte contro la legge nazionale in questione [246], evitando che la sovra-regolamentazione si traduca in oneri normativi o amministrativi per chi utilizza i dati [247]. Un approccio di questo tipo è stato già adottato dal legislatore europeo nello EHDS, che impone agli Stati membri di notificare alla Commissione le misure più rigorose o le garanzie ulteriori introdotte per l'uso secondario di dati genetici, dati provenienti da applicazioni per il benessere e da biobanche, nonché dati molecolari [248].

Anche nel FFR, a fronte del divieto di obblighi di localizzazione dei dati non personali a livello nazionale [249], gli Stati membri che valutano di adottare un progetto di atto in tal senso sono obbligati a darne immeditata comunicazione alla Commissione [250]. In questo modo, si vuole evitare che la presenza di obblighi di localizzazione previsti a livello normativo o nelle prassi amministrative generali degli Stati membri, a meno che non sia giustificata da motivi di sicurezza pubblica e nel rispetto del principio di proporzionalità, provochi problemi di mobilità dei dati, rappresentando un ostacolo alla libertà di stabilimento dei fornitori di servizi di trattamento dei dati, nonché alla loro libertà di fornire i suddetti servizi [251].

In conclusione, le proposte qui formulate mirano a contribuire al raggiungimento di un giusto equilibrio tra l'elevato livello di tutela delle persone fisiche e la libera circolazione dei dati personali. In passato, il legislatore europeo è stato capace di decisioni di questo tipo. Con la direttiva 2011/24/UE sui

---

[246] Artt. 258 e 260 TFUE. Una simile azione non si è ancora verificata sebbene già nel 2017 la Commissione stessa avesse dichiarato il proprio impegno a monitorare "scrupolosamente il modo in cui gli Stati membri applicheranno le clausole specifiche del regolamento generale sulla protezione dei dati, ad esempio per quanto riguarda i dati genetici, biometrici e le informazioni relative alla salute, per garantire che all'interno dell'Unione la libera circolazione dei dati personali non venga indebitamente limitata". Cfr. Comunicazione della Commissione sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, COM(2017) 228 final, del 10 maggio 2017.

[247] In senso analogo, anche nella Comunicazione sull'individuazione e l'eliminazione delle barriere del mercato unico, la Commissione ha richiesto agli Stati membri di comunicare l'eventuale scelta di aggiungere elementi che non derivano dalla legislazione dell'Unione. Questi elementi possono infatti rappresentare oneri normativi o amministrativi ulteriori per i consumatori e le imprese, incidendo in particolare sulle piccole e medie imprese (Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Individuare e affrontare le barriere al mercato unico, COM (2020) 93 final, del 10 marzo 2020).

[248] Art. 51, par. 3, e considerando 52 EHDS.

[249] Art. 4, par. 1, e considerando 4 FFR.

[250] Art. 4, par. 1, e considerando 22 FFR.

[251] Considerando 3 FFR.

diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, ad esempio, in reazione agli orientamenti della Corte [252], sono state introdotte delle disposizioni volte a bilanciare il diritto del paziente di ottenere il rimborso per l'assistenza sanitaria ricevuta all'estero e il legittimo interesse dello Stato di affiliazione a mantenere la stabilità finanziaria del sistema sanitario nazionale e garantire servizi di qualità accessibili su base universale [253].

Paradigmatico in tal senso è l'art. 8, par. 2, direttiva 2011/24/UE che, individuando i casi in cui il rimborso all'assistenza sanitaria può essere subordinato a un'autorizzazione preventiva [254], è stato elaborato nella consapevolezza

---

[252] A fronte della scarsa propensione degli Stati membri a trasporre nei propri ordinamenti i principi enucleati dalla Corte nella giurisprudenza sulla mobilità dei pazienti, infatti, le istituzioni europee hanno avviato delle iniziative legislative, inizialmente di *soft law* e successivamente con efficacia vincolante, che hanno portato all'adozione della direttiva 2011/24/UE. Cfr. F. COSTAMAGNA, *I servizi socio-sanitari nel mercato interno europeo*, Edizioni Scientifiche Italiane, Napoli, 2011, p. 185 ss.

[253] Si veda, in particolare, l'art. 8 e considerando 11-12 direttiva 2011/24/UE.

[254] L'art. 8, par. 2, direttiva 2011/24/UE stabilisce il criterio per ritenere ammissibile l'obbligo di autorizzazione preventiva, senza fare distinzione tra cure ospedaliere e non. Tale criterio si basa sulla necessità di pianificazione da parte delle autorità nazionali per assicurare "un accesso sufficiente e permanente a una gamma equilibrata di cure di elevata qualità", "il controllo dei costi" e la prevenzione di sprechi di "risorse finanziarie, tecniche e umane". Questo obbligo si presume giustificato quando il trattamento in questione: i) comporta il ricovero del paziente per almeno una notte, o ii) richiede l'utilizzo di un'infrastruttura sanitaria e di apparecchiature mediche altamente specializzate e costose. Ad ogni modo, l'obbligo di autorizzazione preventiva deve essere limitato "a quanto necessario e proporzionato e non può costituire un mezzo di discriminazione arbitraria o un ostacolo ingiustificato alla libera circolazione di pazienti, servizi o merci" (art. 8, par. 1, direttiva 2011/24/UE). Inoltre, lo Stato membro non può rifiutare l'autorizzazione "quando l'assistenza sanitaria in questione non può essere prestata sul suo territorio entro un termine giustificabile dal punto di vista clinico, sulla base di una valutazione medica oggettiva dello stato di salute del paziente, dell'anamnesi e del probabile decorso della sua malattia, dell'intensità del dolore e/o della natura della sua disabilità al momento in cui la richiesta di autorizzazione è stata fatta o rinnovata" (art. 8, par. 5, direttiva 2011/24/UE). Le decisioni concernenti l'autorizzazione e il rimborso delle spese devono essere basate sullo stato di salute specifico del paziente e sull'"urgenza del caso e delle singole circostanze" (art. 9, par. 3, direttiva 2011/24/UE). Tali decisioni devono essere motivate, soggette a revisione e impugnabili con ricorso giurisdizionale effettivo. Infine, l'art. 8, par. 6, direttiva 2011/24/UE individua i motivi di diniego per cui le autorità nazionali possono rifiutare di concedere l'autorizzazione, in particolare quando "l'assistenza transfrontaliera può esporre il paziente o il pubblico a un rischio che prevale sull'interesse del paziente a ricercare l'assistenza sanitaria transfrontaliera" (considerando 45 direttiva 2011/24/UE). Per un'analisi critica della disposizione in oggetto, si rinvia a F. COSTAMAGNA, *op. cit*., 2011, p. 195 ss. Per un approfondimento più ampio sulla direttiva 2011/24/UE, invece, cfr. G. DI FEDERICO, S. NEGRI, *op. cit*., 2019, p. 183; G. DI FEDERICO, *Access to Healthcare in the Post-Lisbon Era and the Genuine Enjoyment of EU Citizens' Rights*, in L.S. ROSSI, F. CASOLARI (eds.), *The EU After Lisbon: Amending or Coping with the Existing Treaties*, Springer, Cham, 2014, pp. 177-214; P. QUINN, P. DE HERT, *The European Patients' Rights Directive: A Clarification and*

politica che il rischio di perdere il modello di *welfare state* sarebbe stato talmente elevato da non poter permettere che simili questioni venissero lasciate ai test di proporzionalità della Corte [255]. Difatti, la scelta di garantire un diritto individuale assoluto alla mobilità sanitaria avrebbe avuto effetti devastanti sulla sostenibilità di gran parte dei sistemi sanitari europei e quindi sull'interesse della collettività a garantirsi cure ispirate ai principi dell'universalismo e della solidarietà sociale [256].

Nel caso del GDPR, se matura la consapevolezza che il rischio di non riuscire a curare i singoli individui in modo personalizzato ed efficace è altrettanto elevato senza l'utilizzo dei dati, allora forse il legislatore europeo troverà il coraggio, come sembra aver fatto con lo EHDS, di comprimere *ex lege* alcune delle prerogative riservate agli interessati in nome di una visione più ampia di beneficio collettivo.

3.2. La verifica della compatibilità del diritto nazionale di applicazione del GDPR con il diritto dell'Unione

L'inerzia o, piuttosto, la mancanza di volontà politico-istituzionale del legislatore europeo di mettere mano alle disposizioni più controverse del GDPR non impedisce di valutare, nel frattempo, la possibilità di superare gli ostacoli alla libera circolazione dei dati personali, avviando processi di riforma delle leggi nazionali di applicazione del GDPR. Tali processi potrebbero essere innescati sottoponendo queste norme al vaglio della Corte: qualora, ad esempio, un giudice nazionale, davanti al quale è presentato un ricorso avverso una decisione giuridicamente vincolante dell'autorità di controllo [257], nutrendo dubbi sulla compatibilità di una norma nazionale con il diritto dell'Unione,

---

Codification of Individual Rights relating to Cross Border Healthcare and Novel Initiatives Aimed at Improving Pan-European Healthcare Cooperation, in *Medical Law International*, 2012, vol. 12, n. 1, p. 28.

[255] La necessità di un intervento organico nel settore è stata riconosciuta dagli Stati membri nella "ferma convinzione che in questo settore l'evoluzione [dovesse] derivare da un consenso politico e non prettamente dalla giurisprudenza". Cfr. Dichiarazione sui valori e sui principi comuni, allegata alle Conclusioni del Consiglio sui valori e sui principi comuni dei sistemi sanitari dell'Unione europea, 2 giugno 2006, p. 2.

[256] E. SZYSZCZAK, *Modernising Healthcare: Pilgrimage for the Holy Grail?*, in M. KRAJEWSKI, U. NEERGARD, J.W. VAN DE GRONDEN (eds.), *The Challenging Legal Framework for Services of General Interest in Europe. Between Competition and Solidarity*, TMC Asser Press, The Hague, 2009, p. 200 e C. NEWDICK, *The European Court of Justice, Trans-National Health Care and Social Citizenship – Accidental Death of a Concept?*, in *Wis. Int'l L.J.*, 2009, vol. 26, pp. 854-855.

[257] Art. 78 GDPR.

decida di chiedere alla Corte di pronunciarsi, in via pregiudiziale, sull'interpretazione del GDPR [258].

Un simile esame sulla compatibilità di una legge nazionale con il diritto dell'Unione non può dirsi precluso dal fatto che questa disciplina non è né apertamente in contrasto con il GDPR né palesemente in linea con quanto ivi prescritto. Poiché, infatti, manca un'armonizzazione completa a livello europeo, gli Stati membri, nell'esercizio della loro discrezionalità, sono obbligati a "legiferare in modo da non pregiudicare il contenuto e gli obiettivi di tale regolamento" [259]. Questi ultimi, come evidenziato nel capitolo 3, consistono nel mantenere un giusto equilibrio tra la tutela delle persone fisiche rispetto al trattamento dei loro dati personali e gli interessi di terzi e della collettività nell'utilizzo e nella condivisione di tali dati.

Di conseguenza, le leggi nazionali che impongono il rispetto di requisiti supplementari per il trattamento dei dati personali, compresi quelli sensibili – non previsti dal GDPR – sono suscettibili di contestazione. A questo proposito, un esempio significativo è rappresentato dal Codice della privacy italiano, che presenta vari profili di incompatibilità con il GDPR sia nei casi di trattamento dei dati puramente "interni" sia in quelli con una componente transfrontaliera. In particolare, la previsione di condizioni come il regime autorizzatorio per i trattamenti ulteriori di dati personali per finalità di ricerca medica, biomedica ed epidemiologica costituisce un onere amministrativo aggiuntivo che può provocare ritardi nella conduzione dell'attività di ricerca e,

---

[258] Com'è noto, nell'ambito di un procedimento pregiudiziale d'interpretazione *ex* art. 267 TFUE, la Corte non ha competenza per interpretare le norme di diritto nazionale, e nemmeno per pronunciarsi direttamente sulla loro compatibilità rispetto al diritto dell'Unione. Tuttavia, quest'ultima limitazione viene tradizionalmente superata tramite una formulazione del quesito in modo tale da chiedere se una norma di diritto dell'Unione osta (o non osta) a norme nazionali la cui compatibilità è in dubbio. In questi casi, i giudici di Lussemburgo possono fornire indicazioni sull'interpretazione del diritto dell'Unione così da consentire al giudice *a quo* di procedere a un'interpretazione conforme della normativa nazionale ai requisiti del diritto dell'Unione e, qualora ciò non sia possibile, disapplicare le disposizioni nazionali contrastanti (R. ADAM, A. TIZZANO, *Lineamenti di diritto dell'Unione europea*, Giappichelli, Torino, 2022, pp. 291-292). Sull'importanza del rinvio pregiudiziale quale strumento di dialogo tra la Corte e i giudici nazionali per risolvere questioni di rango costituzionale, v. C. AMALFITANO, *Il futuro del rinvio pregiudiziale nell'architettura giurisdizionale dell'Unione europea*, in *DUE*, 2022, vol. 3-4, pp. 503-509. Per un'ampia disamina sul tema, cfr. F. FERRARO, C. IANNONE, *Il rinvio pregiudiziale*, Giappichelli, Torino, 2020.

[259] Sentenza *Meta Platforms I*, punto 60. In questa occasione, la Corte ha stabilito che il legislatore tedesco ha agito legittimamente entro il margine di discrezionalità offerto dall'art. 80, par. 2, GDPR, poiché il riconoscimento, anche se tramite norme volte a proteggere i consumatori, della legittimazione delle associazioni di tutela dei consumatori ad agire contro violazioni del GDPR assicura la piena realizzazione dell'obiettivo del GDPR di garantire un'efficace protezione dei diritti e delle libertà fondamentali delle persone fisiche (punto 73). In precedenza, ciò era stato affermato, seppur con riferimento alla DPD, nella sentenza *ASNEF*.

conseguentemente, nell'ottenimento di risultati a beneficio della sanità pubblica (sezione 3.2.1), nonché rendere difficile la pianificazione e l'esecuzione di ricerche transfrontaliere (sezione 3.2.2).

3.2.1. (*Segue*) Nelle ipotesi di trattamento puramente "interne"

Per quanto riguarda i trattamenti di dati condotti entro i confini nazionali, un primo profilo di incompatibilità della disciplina italiana riguarda l'art. 110 Codice della privacy che impone l'obbligo di ottenere il consenso per i trattamenti per ricerca medica, biomedica ed epidemiologica che non sono previsti dal diritto dell'Unione o dall'art. 12-*bis*, d.lgs. n. 502/1992, così come per i trattamenti rispetto ai quali informare l'interessato non è impossibile, non implica uno sforzo sproporzionato o non rischia di rendere impossibile/pregiudicare gravemente il conseguimento delle finalità di ricerca. La scelta di prevedere il consenso quale presupposto giuridico per questo tipo di trattamento non sembra tenere conto della *ratio* sottesa né all'art. 9, par. 2, lett. j), GDPR, eccezione volta a favorire la ricerca scientifica, né all'art. 9, par. 4, GDPR che, sebbene permetta allo Stato membro di introdurre "condizioni" o "limitazioni" al trattamento, non legittima l'introduzione di una nuova base giuridica rispetto a quelle prescritte dal GDPR.

Tra l'altro, come sottolineato nel capitolo 3, il consenso rappresenta solo una delle basi giuridiche a cui ricorrere e non necessariamente la più adatta [260]. L'acquisizione del consenso, infatti, può rappresentare un'operazione estremamente onerosa e complessa che, specialmente in alcuni casi, può rendere oltremodo gravoso, se non addirittura impossibile, l'esercizio di un'attività tramite la quale trovano attuazione nell'ordinamento nazionale (e sovranazionale) diritti e valori fondamentali, come il diritto alla salute. Secondo il Centro di Coordinamento Nazionale dei Comitati Etici Italiano (CCNCE), ad esempio, soprattutto in caso di ricerche di tipo osservazionale, dovrebbe potersi fare ricorso a "basi giuridiche alternative per agevolare il (ri)trattamento dei dati *de quibus*, senza dovere ogni volta dipendere da un nuovo consenso dell'interessato – con l'unico limite di una preventiva idonea pseudonimizzazione/cifratura dell'identità del paziente – venendosi così a contemperare ragionevolmente ed efficacemente diritto dell'individuo e interesse della collettività" [261].

---

[260] Più precisamente, sezione 3.1.2 del capitolo 3.

[261] CCNCE, Ricerca osservazionale: un pilastro nel processo di produzione di conoscenza, emessa il 26 luglio 2022 nel contesto del decreto ministeriale del 30 novembre 2021, Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto

Ridurre la centralità del consenso nella disciplina italiana sulla protezione dei dati personali sarebbe coerente con i più recenti sviluppi normativi in materia di uso secondario dei dati sanitari. Con lo EHDS, infatti, si registra un tendenziale spostamento di attenzione dal consenso ai motivi di interesse pubblico e di legittimo interesse come presupposti giuridici dell'attività di trattamento del titolare [262], da combinare con i motivi di interesse pubblico nel settore della sanità pubblica [263] o con finalità di ricerca scientifica [264]. In questa stessa direzione si stanno muovendo, anche se in modo non del tutto coordinato, alcuni Stati membri che, sull'esempio francese, hanno istituito sistemi di governance dei dati (accentrati o decentrati) con il precipuo obiettivo di favorire l'uso secondario degli stessi, specialmente in settori dove gli effetti positivi per la collettività appaiono maggiori [265].

Sempre con riferimento all'art. 110 Codice della privacy, prima delle modifiche apportate dal d.l. n. 19/2024, risultava problematico l'obbligo per il titolare di sottoporre il programma di ricerca alla preventiva consultazione del Garante ai sensi dell'art. 36 GDPR. In particolare, l'avvio di questa procedura comportava un allungamento dei tempi necessari per iniziare gli studi, specialmente se si considera che spesso il termine delle 8 settimane entro cui il

---

legislativo 14 maggio 2019, n. 52, che ammette un passaggio di titolarità *ex lege* tra il titolare del trattamento (ossia il promotore che detiene la chiave di conversione dei dati pseudonimizzati) e il cessionario dei dati e dei risultati di sperimentazioni cliniche senza scopo di lucro a fini registrativi (art. 3, par. 5).

[262] Artt. 6, par. 1, lett. e) e lett. f), GDPR.

[263] Art. 9, par. 2, lett. i), GDPR.

[264] Art. 9, par. 2, lett. j), GDPR.

[265] In Finlandia, con il *Secondary use of health and social data* del 26 aprile 2019 viene istituito un sistema di governance in cui Findata è individuata come autorità nazionale – direttamente subordinata al *Ministry of Social Affairs and Health* – preposta a gestire le richieste di accesso ai dati sanitari presenti nel catalogo nazionale di metadati per finalità di ricerca (e altre finalità, tra cui anche attività di sviluppo e innovazione). Nel processo di accesso ai dati, l'autorità di controllo nazionale non ha alcun ruolo; è infatti Findata a valutare le domande, che possono essere sottoposte a verifica da parte dei comitati etici del *Finnish Institute for Health and Welfare* (non per i "*purely register-based studies*"), e a decidere, entro tre mesi, se concedere il "*data permit*" ai progetti di ricerca, per cui non si prevede una pubblicazione in un registro pubblico. I dati vengono messi a disposizione entro 60 giorni, a seconda dei tempi necessari per il processo di estrazione degli stessi. Non viene specificato se ciò avvenga in un ambiente di trattamento sicuro o meno. Per un approfondimento sulle norme finlandesi circa l'uso secondario dei dati, si veda M. KRUUS, *The Public Interest Requirement in the Secondary Use of Health Data in Scientific Research: The Examples of Estonia and Finland*, in *Juridica International*, 2023, n. 32, pp. 64-73. Per ulteriori esempi di sistemi di governance dei dati per uso secondario a livello nazionale, cfr. *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, 2021, pp. 101-106; F. LUPIÁÑEZ-VILLANUEVA et al., *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, 2021, pp. 175-179.

Garante avrebbe dovuto fornire un riscontro non veniva rispettato. Inoltre, la procedura richiedeva adempimenti particolarmente onerosi per i ricercatori, come la redazione di una DPIA ai sensi dell'art. 35 GDPR, con conseguenti difficoltà pratiche e amministrative che rallentavano ulteriormente la fase iniziale delle ricerche.

Oltre a questo tipo di problemi di ordine pratico, tale requisito contrastava con il dettato normativo del GDPR per vari motivi. In primo luogo, l'automatismo previsto dalla legge italiana, che imponeva l'attivazione della procedura di consultazione preventiva a prescindere dall'esito della DPIA e, in particolare, dalla sussistenza di un rischio residuo elevato non mitigabile dal titolare, non risultava giustificato dalla *ratio* della normativa in questione. Al contrario, nel GDPR la consultazione preventiva dell'autorità di controllo viene richiesta esclusivamente nei casi in cui permanga un rischio residuo elevato non mitigabile [266] oppure qualora il diritto nazionale stabilisca la necessità di una consultazione finalizzata all'ottenimento di un'autorizzazione preliminare, ma limitatamente ai trattamenti effettuati per l'esecuzione di un compito di interesse pubblico, quali quelli in ambito di sanità pubblica [267].

In secondo luogo, la scelta del legislatore italiano di prevedere come automaticamente obbligatoria la consultazione preventiva davanti al Garante non poteva ritenersi giustificata nemmeno in virtù dell'art. 36, par. 5, GDPR, poiché questa disposizione non consente allo Stato membro di prevedere l'*obbligo* di consultazione preventiva per *qualsiasi* trattamento. Piuttosto, essa fornisce la possibilità al diritto nazionale di prescrivere una consultazione preventiva davanti all'autorità di controllo per l'ottenimento di un'autorizzazione preliminare nel caso in cui il titolare sia incaricato di svolgere un compito di interesse pubblico. In deroga al principio di *accountability*, cuore dell'art. 35 GDPR, il diretto coinvolgimento dell'autorità di controllo di cui all'art. 36, infatti, è pensato unicamente per sopperire alle mancanze del titolare nell'eliminare i rischi connessi alla sua attività di trattamento, tramite l'adozione di misure di sicurezza adeguate, specialmente se caratterizzata da una particolare

[266] Art. 36, par. 1, e considerando 94 GDPR.

[267] Ai sensi dell'art. 36, par. 5, GDPR, "il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica". Nel Codice della privacy, tale disposizione è stata attuata tramite l'art. 2-*quinquiesdecies* in cui si afferma che "[c]on riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati ai sensi dell'art. 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare è tenuto ad adottare".

complessità, come quelle necessarie per eseguire un compito di interesse pubblico [268].

In terzo luogo, la previsione della consultazione preventiva implicava l'obbligo di svolgere una DPIA, indipendentemente dal soddisfacimento delle condizioni richieste dal GDPR, ossia che il trattamento comporti un "rischio elevato per i diritti e le libertà delle persone fisiche", per via dell'utilizzo di nuove tecnologie e della natura, oggetto, contesto e finalità del trattamento [269]. Al contrario, la maggior parte degli studi condotti per finalità di ricerca medica, biomedica ed epidemiologica – in particolare se retrospettivi – non richiede l'utilizzo di "nuove tecnologie" (ad es. algoritmi che, ormai, sono largamente diffusi nella rielaborazione dei dati in ambito medico-scientifico) [270] e non comporta necessariamente un impatto sulla salute dei pazienti o sulla loro riservatezza. Ciò vale soprattutto per le ricerche effettuate nel rispetto dell'art. 32 GDPR, che prevede l'utilizzo di dati in forma pseudonimizzata [271].

Passando all'analisi dell'art. 110-*bis* Codice della privacy, a sollevare dubbi di compatibilità con il GDPR è il potere conferito al Garante di bloccare il riutilizzo dei dati per fini di ricerca. Difatti, la mancata pronuncia sull'autorizzazione al trattamento ulteriore entro il termine di 45 giorni dalla richiesta equivale a un rigetto [272], una forma di "silenzio diniego" che nel diritto amministrativo nazionale rappresenta un'eccezione alla regola generale del "silenzio assenso" [273]. In questo modo, il Garante viene dotato di un potere autorizzatorio, non previsto dalla normativa europea, che può portare anche alla decisione di bloccare un trattamento dei dati, perfino nell'ipotesi in cui,

---

[268] A. MANTELERO, *Consultazione preventiva*, in R. D'ORAZIO et al., *op. cit.*, 2021, p. 552.

[269] Art. 35, par. 1, GDPR. Inoltre, il terzo paragrafo della medesima disposizione contiene un elenco esemplificativo dei trattamenti che potrebbero comportare una DPIA, come quelli su larga scala di categorie particolari di dati personali di cui all'art. 9, par. 1, GDPR. Cfr. WP, Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento (UE) 2016/679, WP 248 rev.01, 2017.

[270] Sul punto, sono particolarmente interessanti le considerazioni espresse nella sentenza del 15 dicembre 2022, n. 416 dal Tribunale di Udine, che ha esaminato il caso in cui l'AUSL Friuli Centrale ha impugnato il provvedimento del Garante (doc. web n. 9845156). Questo provvedimento contestava l'illiceità del trattamento dei dati personali contenuti nelle banche dati aziendali e nel FSE mediante l'utilizzo di un algoritmo denominato ACG da parte di una società *in-house* della Regione (Insiel SPA). L'algoritmo ACG era impiegato per realizzare un profilo sanitario di rischio con riferimento alle patologie che potevano esporre gli assistiti più fragili a contrarre infezioni più gravi da Covid-19.

[271] Cfr. https://www.studiolegalestefanelli.it/it/approfondimenti/le-nuove-regole-privacy-per-gli-studi-retrospettivi-la-vittoria-dellaccountability-nella-ricerca-scientifica.

[272] Art. 110-*bis*, par. 2, Codice della privacy.

[273] Art. 20 l. del 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

ad esempio, questo abbia ottenuto parere favorevole da parte del comitato etico territorialmente competente.

Tale previsione contrasta con la scelta del legislatore europeo di privilegiare un intervento preventivo basato su una maggiore responsabilizzazione dei titolari e dei responsabili del trattamento. Nel GDPR, infatti, il potere autorizzatorio delle autorità di controllo rimane circoscritto ai casi di trasferimenti di dati personali oltre i confini dell'Unione [274] e quando gli Stati membri decidono di prevederlo in relazione allo svolgimento di compiti di pubblico interesse [275]. In quest'ottica, il potere di vietare di procedere al trattamento dovrebbe rappresentare un'ipotesi eccezionale, da applicare solo quando il titolare e l'autorità concludono che non esistono misure sufficienti per salvaguardare i diritti e le libertà degli interessati [276].

In conclusione, per come attualmente redatti, gli artt. 110 e 110-*bis* Codice della privacy non sembrano consentire una ragionevole ponderazione tra il diritto alla protezione dei dati personali di cui all'art. 8 della Carta e gli interessi generali perseguibili tramite lo svolgimento di attività di ricerca scientifica [277]. Ciò risulta ancor più vero se si considera che le decisioni del Garante in ambito sanitario sono tutte sistematicamente penalizzanti per qualsiasi uso ulteriore dei dati, talvolta anche in situazioni in cui non ci sono rischi elevati per i diritti degli interessati [278]. Oltre a determinare un rallentamento delle attività scientifiche, in Italia si assiste a un vero e proprio "*chilling effect*", con alcuni titolari che scelgono di non avviare progetti a causa dell'incertezza riguardo alla possibilità di (ri-)utilizzare i dati raccolti [279].

Questa situazione potrebbe tradursi anche in un livello di qualità nelle cure erogate ai cittadini italiani inferiore rispetto a quello garantito in altri Stati

---

[274] Artt. 46, par. 3, 57, par. 1, lett. r) e 58, par. 3, lett. i), GDPR. Per una trattazione complessiva sul tema dei trasferimenti di dati a Paesi extra-UE, cfr. G. RUGANI, *La regolamentazione dei flussi di dati personali dall'UE verso Paesi terzi. Alla ricerca di un bilanciamento tra espansione del commercio internazionale e* personal data protection, Giappichelli, Torino, 2024.

[275] Artt. 36, par. 3, e 58, par. 3, lett. c), GDPR.

[276] Art. 58, par. 2, lett. f), GDPR.

[277] Ponderazione che, invece, è richiesta non solo dallo stesso art. 9, par. 2, lett. j), GDPR, ma anche dagli artt. 8, parr. 2-3, e 52, par. 1, Carta.

[278] Oltre ai casi menzionati nelle sezioni precedenti, si vedano le altre pronunce pubblicate sul sito ufficiale del Garante https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica.

[279] Nel *workshop* sul GDPR e sull'uso secondario dei dati organizzato da EMA nel 2020, è stato rilevato che "*[n]ew projects are not even undertaken because the stakeholders fear to be blocked by GDPR concerns*". Cfr. https://www.ema.europa.eu/en/documents/presentation/presentation-academia-feedback-general-data-protection-regulation-gdpr-secondary-data-use_en.pdf. Considerazioni simili sono state svolte anche in dottrina da, *inter alia*, R. BECKER et al., *Purpose Definition as a Crucial Step for Determining the Legal Basis under the GDPR: Implications for Scientific Research*, in *JLB*, 2024, pp. 3-4.

membri. Le restrizioni all'uso dei dati rischiano infatti di rallentare lo sviluppo di tecnologie avanzate di IA in grado, ad esempio, di rilevare la presenza di un cancro a uno stadio precoce. Nello scenario ipotizzato, i cittadini europei potrebbero beneficiare di standard di cura significativamente diversi a seconda delle scelte operate dallo Stato di affiliazione nel bilanciamento tra il diritto alla protezione dei dati e il diritto al trattamento dei dati per finalità di interesse generale [280].

Al fine di rendere la disciplina italiana maggiormente in linea con i "veri" obiettivi del GDPR, la strada preferibile sarebbe una riformulazione degli artt. 110 e 110-*bis* Codice della privacy. Per quanto riguarda l'art. 110, sarebbe opportuno abbandonare l'approccio consenso-centrico per l'uso dei dati ai fini di ricerca scientifica, modificando tale previsione in modo da consentire il ricorso a basi giuridiche alternative (*in primis*, l'interesse pubblico). Inoltre, nonostante l'eliminazione del requisito della consultazione preventiva, è bene che la sistematizzazione delle garanzie già adottate dal Garante ai sensi dell'art. 106, par. 2, lett. d), Codice della privacy non venga effettuata in modo da richiedere sforzi eccessivi al titolare del trattamento.

Con riferimento all'art. 110-*bis* Codice della privacy, il potere attribuito al Garante di bloccare il riutilizzo dei dati per finalità di ricerca dovrebbe essere eliminato, sostituendo la regola del silenzio-rigetto con quella del silenzio-assenso. Più in generale, si impone un ripensamento complessivo della norma, anche alla luce della sua scarsa applicazione pratica [281] e delle ambiguità interpretative.

In particolare, l'attuale formulazione solleva rilevanti incertezze concettuali. La rubrica e i primi tre paragrafi dell'art. 110-*bis* Codice della privacy fanno infatti riferimento al "trattamento ulteriore da parte di terzi", espressione che non trova un corrispettivo nel testo del GDPR, dove il "trattamento ulteriore" concerne l'uso dei dati da parte del medesimo titolare per finalità diverse rispetto a quelle originarie. Al contrario, la situazione disciplinata dalla norma italiana sembra riguardare un riutilizzo da parte di soggetti terzi, ossia un uso secondario, che pone questioni distinte sul piano della compatibilità delle finalità.

---

[280] Il caso fornito tende a semplificare, per finalità esplicative, una situazione che nella realtà si presenta molto più complessa. Infatti, la possibilità per un paziente di beneficiare di questi sistemi di IA non è legata solamente al regime normativo di maggiore o minore favore per la ricerca scientifica, ma anche alle scelte di politica sanitaria dei singoli Stati membri.

[281] L'art. 110-*bis* Codice della privacy è stato poco utilizzato nella prassi dal momento che è invalso l'orientamento secondo cui l'art. 110 Codice della privacy si configura quale *lex specialis* rispetto all'art. 110-*bis*, in quanto circoscritto ai soli trattamenti di dati sanitari effettuati per finalità di ricerca medica, biomedica ed epidemiologica.

Da questo punto di vista, desta particolare perplessità la previsione di cui al quarto paragrafo, relativo agli IRCCS. Qualora tali istituti trattino dati raccolti da altri soggetti, non appare giustificata l'automatica applicazione della presunzione di compatibilità tra finalità originaria e finalità di ricerca solo in ragione della missione istituzionale degli IRCCS. Una simile presunzione ignora la concreta discontinuità tra soggetti e scopi del trattamento, introducendo un'eccezione difficilmente giustificabile e potenzialmente in contrasto con il principio di eguaglianza sostanziale, con il rischio di configurarsi come misura di dubbia legittimità costituzionale [282].

3.2.2. (*Segue*) Nelle ipotesi di trattamento a carattere transfrontaliero

Confrontando la disciplina italiana con quella di altri Stati membri, emergono ulteriori profili di incompatibilità nelle ipotesi di trattamento transfrontaliero di dati personali. Come già ricordato, le "ulteriori condizioni, comprese limitazioni", previste dal diritto nazionale riguardo al trattamento di dati genetici, biometrici o relativi alla salute ai sensi dell'art. 9, par. 4, GDPR non possono rappresentare un ostacolo alla libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi [283]. Tuttavia, la scelta del legislatore italiano di subordinare il trattamento dei dati personali a fini di ricerca al consenso e, nel caso di trattamento ulteriore, alla sua autorizzazione potrebbe costituire un ostacolo alla libera circolazione dei dati [284], e con essa, alla collaborazione tra ricercatori europei [285].

Consideriamo, ad esempio, un ipotetico studio multicentrico tra gruppi di ricerca afferenti a organizzazioni stabilite in più Stati membri (ad es. Italia e Francia) per analizzare retrospettivamente dati clinici archiviati presso i diversi centri con finalità di ricerca epidemiologica. Nel caso ipotizzato, essendo particolarmente complicato ottenere il consenso per gli studi retrospettivi, i ricercatori italiani sono sostanzialmente obbligati a coinvolgere il Garante in via consultiva (situazione precedente alla modifica del d.l. n. 19/2024) o, in caso di trattamento ulteriore, autorizzatoria. Al contrario, in Francia, non è richiesta la consultazione preventiva della CNIL, fatto salvo il caso di

---

[282] Come rilevato da G. COMANDÉ, *Ricerca in sanità e data protection un puzzle… risolvibile*, in *Rivista italiana di medicina legale*, 2019, fasc. 1, p. 202, suscita perplessità il regime differenziato previsto dall'art. 110-*bis*, par. 4, Codice della privacy per gli IRCCS e non, invece, per le strutture che si occupano sia di assistenza sanitaria sia di ricerca (ad es. le aziende ospedaliere universitarie).

[283] Considerando 53 GDPR.

[284] Art. 16, par. 2, TFUE e art. 1, par. 3, GDPR.

[285] Art. 179, par. 2, TFUE.

rischio residuo, e il regime autorizzatorio viene mitigato dalla possibilità per il titolare del trattamento di fornire all'autorità di controllo una dichiarazione di conformità alle MR [286]. Inoltre, in Italia, la forma di "silenzio diniego" di cui all'art. 110-*bis* Codice della privacy può risultare problematico se si pensa che, nel sistema francese, la mancata autorizzazione da parte della CNIL entro due mesi dalla presentazione della domanda di accesso ai dati, già verificata dall'HDH e dal comitato etico competente, non equivale a un rigetto, bensì a un accoglimento.

Pur non privando i ricercatori italiani della possibilità di trattare i dati, le disposizioni del Codice della privacy subordinano lo svolgimento delle attività di ricerca a requisiti supplementari che, se non soddisfatti, ne impediscono *de facto* la realizzazione. In questo modo, le norme italiane finiscono non solo per rendere più complessa e onerosa la procedura da seguire per l'uso dei dati per tali finalità, ma finiscono anche per scoraggiare i ricercatori di altri Stati membri dall'avviare attività di ricerca collaborativa che richiede lo scambio di dati con l'Italia, poiché rischiano di veder rallentata la loro attività. In ragione di questo effetto dissuasivo, si può sostenere che gli artt. 110 e 110-*bis* Codice della privacy ostacolino, anche solo indirettamente [287], la libera

[286] Un altro esempio significativo, accanto alla Francia, di Stato all'avanguardia nelle scelte normative che facilitano l'utilizzo dei dati per determinate finalità è rappresentato dalla Finlandia. Il *Data Protection Act* (1050/2018) non prevede l'obbligo di ottenere l'autorizzazione dell'autorità di controllo in assenza del consenso dell'interessato. Per l'impiego di dati sanitari a fini di ricerca (sezione 4, par. 1, n. 3 e sezione 6, par. 1, n. 7), è richiesto al titolare del trattamento di "*take suitable and specific measure to safeguard the rights of the data subject*", tra cui la designazione di un DPO, la pseudonimizzazione, la DPIA o altre misure tecniche, procedurali e organizzative (sezione 6, par. 2). Inoltre, la redazione di una DPIA è obbligatoria anche nel caso in cui vengano introdotte deroghe ai diritti degli interessati previsti dagli artt. 15, 16, 18 e 21 del GDPR. Qualora il trattamento riguardi dati relativi alla salute, oltre alle garanzie previste *ex lege* (sezione 31, parr. 1 e 2), la DPIA deve essere trasmessa all'autorità di controllo (*Finnish Data Protection Ombudsman*), esclusivamente a titolo informativo. In alternativa, è possibile dimostrare la conformità a un codice di condotta (sezione 31, par. 3). In caso di uso secondario, si rimanda a quanto descritto nella nota 265.

[287] Secondo la nota formula Dassonville, in materia di libera circolazione delle merci, una norma nazionale integra l'ipotesi di misura di effetto equivalente a restrizioni quantitative qualora sia idonea "ad ostacolare, direttamente o indirettamente, in atto o in potenza, gli scambi intracomunitari" (sentenza della Corte dell'11 luglio 1974, causa C-8/74, *Dassonville*, ECLI:EU:C:1974:82, punto 5). Si ricordi, altresì, il termine "restrizione" è stato interpretato estensivamente nella giurisprudenza della Corte relativa alla libera circolazione delle merci (sentenza della Corte del 20 febbraio 1979, causa C-120/78, *Rewe-Zentral*, ECLI:EU:C:1979:42, p. 649) e dei servizi (sentenze della Corte del 5 ottobre 2010, causa C-173/09, *Elchinov*, ECLI:EU:C:2010:581, punto 41; del 19 aprile 2007, causa C-444/05, *Stamatelaki*, ECLI:EU:C:2007:231, punti 26-28; del 16 maggio 2006, causa C-372/04, *Watts*, ECLI:EU:C:2006:325, punti 96-98; del 13 maggio 2003, causa C-385/99, *Müller-Fauré e van Riet*, ECLI:EU:C:2003:270, punti 41-46; del 12 luglio 2001, causa C-157/99, *Smits e Peerbooms*, ECLI:EU:C:2001:404, punti 61-69; del 28 aprile 1998, *Kohll*, ECLI:EU:C:1998:171, punti 34-35).

circolazione dei dati personali ai sensi dell'art. 16 TFUE e dell'art. 1, par. 3, GDPR, nonché la cooperazione tra ricercatori a livello transfrontaliero ai sensi dell'art. 179, par. 2, TFUE.

Inoltre, in prospettiva, queste disposizioni risultano problematiche rispetto alle norme dello EHDS sull'uso secondario dei dati sanitari. A questo proposito, occorre rilevare che, ancor prima dell'entrata in vigore dello EHDS, alcuni Stati membri, anche se in modo non del tutto coordinato, si sono già adoperati in questo senso. In particolare, Francia e Finlandia hanno ispirato molte delle disposizioni del regolamento europeo grazie all'istituzione di modelli di *data governance*, sia centralizzati che decentralizzati, pensati per semplificare l'uso dei dati sanitari [288].

Anche la Germania ha adottato una legge sull'utilizzo dei dati sanitari a fini di ricerca, miglioramento dell'assistenza sanitaria e altri scopi di interesse pubblico (*Gesundheitsdatennutzungsgesetz*, GDNG) [289]. Tale intervento normativo risponde all'esigenza di superare la frammentazione e la scarsa disponibilità di dati di qualità e rappresentativi, anche nell'ottica di prepararsi alla fase di attuazione dello EHDS [290]. La legge ha istituito un Ufficio per l'accesso e il coordinamento dei dati sanitari presso il BfArM (Istituto federale per farmaci e dispositivi medici), al quale sono attribuiti diversi compiti, tra cui la gestione di un catalogo pubblico di metadati dove sono raccolti i dati sanitari disponibili nel sistema sanitario tedesco e la valutazione delle domande di accesso presentate dai titolari dei dati [291].

Attualmente, in Italia, mancano interventi normativi di questo tipo. Gli unici sviluppi rilevanti sono legati alla transizione digitale promossa dal PNRR, e riguardano, da un lato, il FSE e, dall'altro, l'Ecosistema dei Dati Sanitari (EDS) [292]. Dopo i pareri negativi del Garante su entrambi gli schemi

---

[288] Per quanto riguarda la Francia, si rinvia all'analisi svolta nella sezione 2.1.2 della presente analisi. Con riferimento, invece, alla Finlandia, v. note 255 e 286.

[289] L. del 25 marzo 2024, n. 102, *Gesundheitsdatennutzungsgesetz*, entrata in vigore il 26 marzo 2024. Oltre a questa legge, si segnalano anche la proposta di legge sui dati della ricerca (*Forschungsdatengesetz*, FDG) e la legge sui registri medici (*Registergesetz*).

[290] Spiegazione al GDNG, pp. 1-2.

[291] Sezione 3 GDNG. Altri compiti sono indicati anche nella sezione 4, parr. 4 e 7-8, rispetto alle richieste dei dati dell'*Health Research Data Center*.

[292] L'uso dei dati personali, compresi quelli sanitari, per finalità di ricerca scientifica è inoltre favorito dalla legge del 23 settembre 2025, n. 132, Disposizioni e deleghe del Governo in materia di intelligenza artificiale. L'art. 8 disciplina in modo espresso i trattamenti effettuati per la realizzazione di sistemi di IA con finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicinali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, sanità pubblica, incolumità della persona, salute e sicurezza sanitaria. La norma qualifica tali trattamenti come di rilevante interesse pubblico, con la conseguenza che la base giuridica applicabile

di decreti del Ministero della Salute [293], il Governo italiano ha scelto di dare priorità al decreto relativo al FSE, condizione necessaria per potersi avvalere dei finanziamenti del PNRR. Nel fare ciò, si è però concentrato unicamente sull'uso del FSE per finalità di cura, prevenzione e profilassi internazionale [294], rimandando a data da definirsi un intervento futuro sull'uso dello stesso per finalità di ricerca scientifica e governo sanitario [295]. In origine, il decreto ministeriale sul FSE 2.0 prevedeva che il FSE offrisse "funzioni di estrazione, pseudo-anonimizzazione/anonimizzazione e preparazione di dati" per gli enti di ricerca, consentendo loro di utilizzarli per l'analisi e lo studio delle patologie e delle terapie, nonché dei fattori che hanno incidenza sulla

diventa l'art. 9, par. 2, lett. g), GDPR. L'art. 8 potrebbe dunque costituire la norma nazionale di riferimento richiesta dal GDPR per legittimare questi trattamenti, sebbene permangano alcune incertezze legate all'art. 2-*sexies* del Codice privacy, il quale potrebbe richiedere ulteriori atti normativi o generali per soddisfare il requisito di determinatezza, in linea con le osservazioni formulate dal Garante nel parere del 2 agosto 2024 su uno schema di disegno di legge in materia di IA (doc. web n. 10043532). Benché innovativa, la disposizione presenta infatti diverse criticità. Anzitutto, l'ambito soggettivo non è del tutto chiaro, dal momento che la legge fa riferimento a soggetti pubblici e privati senza scopo di lucro, IRCCS, nonché soggetti privati operanti nel settore sanitario esclusivamente nell'ambito di progetti di ricerca che vedano la partecipazione di soggetti pubblici, privati senza scopo di lucro o IRCCS, senza precisare se la categoria dei soggetti pubblici debba riferirsi in generale alla pubblica amministrazione, oppure ai soli enti pubblici che svolgono ricerca sanitaria, o ancora ai soggetti pubblici senza scopo di lucro. Inoltre, pur ampliando la possibilità di utilizzo, la legge mantiene l'obbligo di comunicare determinate informazioni al Garante, tra cui le misure di sicurezza e la DPIA, riservando all'Autorità un termine di trenta giorni per eventualmente bloccare il trattamento (art. 8, par. 5). Come già evidenziato, tali aspetti non fanno venire meno la portata innovativa della normativa, che – oltre agli aspetti sopra richiamati – consente l'utilizzo dei dati personali precedentemente raccolti e pseudonimizzati, assolvendo agli obblighi informativi anche tramite la sola pubblicazione generale sul sito web del titolare e senza necessità di effettuare la valutazione di compatibilità prevista dall'art. 6, par. 4, GDPR (art. 8, par. 2). La legge introduce inoltre una base giuridica *ad hoc* per i trattamenti finalizzati all'anonimizzazione, alla pseudonimizzazione e alla sintetizzazione dei dati, comprese le categorie particolari, attribuendo ad Agenas il compito di adottare e aggiornare le relative procedure tecniche (art. 8, parr. 3-4). Infine, mentre l'art. 8 riguarda i trattamenti per finalità di ricerca scientifica nella realizzazione di sistemi di IA, la legge italiana contiene anche l'art. 9 che si applica all'insieme dei trattamenti di dati personali – anche secondari – effettuati per finalità di ricerca scientifica e sperimentazione tramite sistemi di IA e tecniche di *machine learning*, includendo altresì le attività svolte all'interno delle *sandbox* regolamentari.

[293] Pareri al Ministero della Salute sullo schema di decreto, da adottare assieme al Ministro delegato per l'innovazione e la tecnologia digitale, di concerto con il Ministro dell'economia e delle finanze, sul FSE (doc. web n. 9802729) e sull'Ecosistema dei Dati Sanitari (doc. web n. 9802752), del 22 agosto 2022.

[294] Artt. 15-19 decreto sul FSE 2.0.

[295] Nelle more, i Capi III e IV del d.p.c.m. n. 178/2015 resteranno in vigore fino al 31 marzo 2026, data in cui troveranno applicazione gli artt. 17-18 del decreto ministeriale sull'EDS.

salute della popolazione [296]. Inoltre, tali enti avrebbero potuto utilizzare i dati presenti nel FSE per addestrare modelli di IA e *machine learning*, con applicazioni in ambito di medicina personalizzata e *value-based healthcare* [297].

Con la recente adozione del decreto ministeriale sull'EDS [298], i soggetti pubblici o privati impegnati in attività di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico possono richiedere l'estrazione di dati anonimizzati nell'ambito dell'EDS, limitatamente però ai dati conferiti al sistema del FSE dalle strutture sanitarie e sociosanitarie, nonché dagli enti del SSN e con esclusione di quelli oscurati ai sensi degli artt. 6 e 9 del decreto sul FSE 2.0 [299]. A tal fine, i soggetti interessati sono tenuti a presentare ad Agenas una richiesta corredata da un progetto di ricerca conforme ai principi metodologici ed etici e, ove previsto, alle regole deontologiche per trattamenti a fini statistici e di ricerca scientifica di cui all'allegato A5 del Codice Privacy e al Provvedimento sulle prescrizioni relative al trattamento di categorie particolari di dati [300].

L'attribuzione ad Agenas di un ruolo centrale nella valutazione delle richieste di estrazione dei dati è in linea con quanto previsto dallo EHDS e con le scelte normative adottate in altri Paesi, come Francia e Finlandia. Tuttavia, questo meccanismo non si estende ad altre finalità, come il governo sanitario, per cui l'accesso a dati pseudonimizzati e aggregati è riservato esclusivamente al personale degli Uffici del Ministero della Salute, di Agenas, e delle regioni e delle province autonome competenti in materia [301]. Analoghe limitazioni si

---

[296] Decreto ministeriale del 20 maggio 2022, Adozione delle Linee guida per l'attuazione del FSE, allegato A, p. 92.

[297] *Ibid.* p. 98.

[298] Decreto del 31 dicembre 2024, Istituzione dell'Ecosistema dati sanitari (decreto sull'EDS). L'adozione di tale decreto è stata possibile solo dopo il parere favorevole del Garante privacy sullo schema di decreto del Ministero della Salute sull'Ecosistema Dati Sanitari (EDS), ai sensi dell'art. 12, comma 15-*quater*, d.l. 18 ottobre 2012, n. 179 (doc. web n. 10062302), 26 settembre 2024, con cui ha ritenuto superate le criticità precedentemente evidenziate nel parere non positivo del 22 agosto 2022.

[299] Art. 3 decreto sull'EDS. Rientrano nell'EDS anche i dati resi disponibili tramite il Sistema Tessera sanitaria.

[300] Art. 17, par. 2, decreto dell'EDS. Tuttavia, ai sensi dell'art. 17, par. 1, decreto sull'EDS, la presentazione di una richiesta ad Agenas non è necessaria quando l'estrazione dei dati per finalità di ricerca è resa disponibile al personale dei competenti Uffici del Ministero della Salute, di Agenas e delle regioni e province autonome.

[301] Art. 16 decreto sull'EDS. L'All. A del medesimo decreto definisce le modalità di accesso differenziate ai servizi dell'EDS in base ai soggetti richiedenti. In particolare, il punto 5 dell'All. A distingue le categorie di utenti e i relativi servizi disponibili: per gli assistiti e i professionisti sanitari, l'accesso all'EDS si limita principalmente alla consultazione dei dati, mentre per le regioni, le province autonome, il Ministero della Salute sono previsti anche servizi di estrazione e analisi dei dati.

riscontrano per le finalità di cura, prevenzione e profilassi internazionale, in relazione alle quali l'accesso ai servizi dell'EDS è consentito solo a categorie specifiche di soggetti [302] e, in ogni caso, subordinato al previo consenso dell'assistito [303]. Una condizione, quest'ultima, che l'EHDS ammette soltanto per determinate tipologie di dati particolarmente sensibili, come quelli genetici o provenienti da applicazioni per il benessere e sperimentazioni cliniche [304].

4. Riflessioni conclusive

Il presente capitolo ha inteso evidenziare come l'effettiva realizzazione di obiettivi quali la libera circolazione dei dati, perseguiti tanto dal GDPR quanto dai regolamenti adottati nell'ambito della Strategia europea del 2020, rischi di essere compromessa per via di questioni connesse principalmente alla "messa a terra" della disciplina sulla protezione dei dati personali. Il confronto tra le normative di attuazione del GDPR in Francia e in Italia, così come tra le prassi amministrative delle rispettive autorità di controllo, ha portato alla luce alcuni limiti del GDPR, rispetto ai quali potrebbe rendersi auspicabile un compromesso politico volto a una sua revisione che non sia esclusivamente orientata a esigenze di competitività.

---

[302] Ad esempio, per le finalità di cura, i servizi di estrazione dei dati sono accessibili alle strutture sanitarie e socio-sanitarie, ai medici convenzionati e agli esercenti le professioni sanitarie che prendono in cura l'assistito, anche al di fuori del SSN (art. 13 decreto sull'EDS). Per le finalità di prevenzione, i servizi elencati all'All. A sono resi disponibili anche alle regioni, alle province autonome e alla Direzione generale competente in materia di prevenzione sanitaria del Ministero della Salute (art. 14 decreto sull'EDS). Infine, per la profilassi internazionale, l'accesso ai servizi è riservato alla Direzione generale competente in materia di profilassi internazionale del Ministero della Salute (art. 15 decreto sull'EDS).

[303] A tale proposito, occorre precisare che, in linea con quanto stabilito dall'art. 10, par. 2, EHDS che consente agli Stati membri di introdurre deroghe all'esercizio del diritto di *opt-out* per l'uso primario, l'art. 18 del decreto sull'EDS prevede specifiche eccezioni. In particolare, in situazioni di impossibilità fisica, incapacità di agire o di intendere e di volere, nonché in caso di rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato che non abbia espresso il consenso al FSE e all'EDS, gli operatori del SSN e dei servizi socio-sanitari regionali, nonché gli esercenti le professioni sanitarie possano accedere prioritariamente al Profilo Sanitario Sintetico e, se necessario, al resto del FSE e ai servizi dell'EDS per finalità di cura (v. anche All. A, punto 4). Inoltre, l'accesso ai dati dell'EDS per finalità di prevenzione da parte delle regioni/province autonome e della Direzione generale competente in materia di prevenzione sanitaria del Ministero della Salute è subordinato all'autorizzazione del Direttore generale della Direzione generale del Ministero della Salute competente in materia di prevenzione sanitaria. Tale accesso è altresì circoscritto ai dati dell'EDS relativi esclusivamente ai soggetti appartenenti a una specifica coorte preventivamente individuata (art. 14, par. 7, decreto sull'EDS).

[304] Art. 51, par. 3, EHDS.

Oltre alle modifiche ipotizzate in relazione al trattamento di dati personali per finalità di ricerca scientifica, alla luce dell'analisi svolta nel capitolo 3, appare opportuno avviare una riflessione per chiarire non solo il concetto di "dato personale", ma anche quello di "trattamento". Un simile intervento contribuirebbe a rafforzare la prevedibilità e la coerenza applicativa del GDPR, senza pregiudicare il livello di tutela garantito agli interessati. Espressioni come "qualsiasi informazione" o "rivelano" – pur coerenti con l'intento garantista della normativa – si prestano, in alcuni contesti, a interpretazioni eccessivamente estensive, che possono generare incertezze applicative. L'obiettivo non è quello di restringere l'ambito di applicazione delle definizioni, bensì di fornire chiarimenti sistematici o criteri interpretativi univoci, che consentano una più uniforme applicazione della disciplina.

In parallelo, risulterebbe auspicabile un ripensamento delle clausole di apertura facoltative contenute nel GDPR. Sebbene concepite per assicurare flessibilità agli Stati membri, tali clausole si sono rivelate spesso fonti di frammentazione normativa, soprattutto in materia di diritti degli interessati. Laddove sia realisticamente possibile raggiungere un consenso tra gli Stati membri, anche alla luce delle differenti tradizioni storiche e normative, una riduzione o eliminazione di tali aperture potrebbe contribuire a contenere la frammentazione, senza indebolire il livello di protezione dei dati personali.

Nonostante siano state recentemente avanzate alcune proposte di semplificazione degli obblighi, soprattutto a beneficio delle piccole e medie imprese, un intervento di revisione di questo tipo implicherebbe l'avvio di un iter legislativo presumibilmente ancora più complesso e controverso di quello che ha condotto all'adozione dell'attuale assetto normativo. Per questa ragione, pur senza abdicare all'idea di una revisione complessiva del GDPR, che si ritiene necessaria almeno per i profili evidenziati, si è indicata come possibile via alternativa – anche solo temporanea – quella di sottoporre al vaglio della Corte la compatibilità delle normative nazionali maggiormente problematiche, in termini di ostacolo alla libera circolazione dei dati, con il diritto dell'Unione europea. Tale via potrebbe contribuire a innescare, almeno indirettamente, un processo di riforma anche a livello nazionale.

In questa eventualità, tuttavia, risulterà cruciale che la Corte adotti un approccio interpretativo capace di ponderare i diritti e gli interessi in gioco, tenendo conto delle esternalità positive che possono derivare per la collettività dall'uso e dalla condivisione dei dati. All'atto di soppesare il diritto dell'interessato alla protezione dei dati personali, non può essere trascurato il fatto che alcune attività di trattamento consentano di dare concreta attuazione a diritti fondamentali e principi generali riconosciuti dall'ordinamento giuridico dell'Unione, come il diritto alla salute [305] e i principi di non discriminazione

[305] Art. 35 della Carta.

e di equo accesso a cure sanitarie di qualità [306], nonché di contribuire alla realizzazione di obiettivi quali la tutela della sanità pubblica [307], della ricerca e del progresso scientifico e tecnologico [308].

In un ordinamento giuridico composito, costituito da regole ed eccezioni, volte a salvaguardare le specificità nazionali in settori "sensibili" come quello sanitario, le operazioni di bilanciamento condotte dagli interpreti e, ancor prima, dal legislatore, risultano decisive per orientare il cammino dell'integrazione europea e contribuire alla costruzione dell'identità dell'Unione [309]. Anche la regolazione dei dati sanitari, per quanto circoscritta a un ambito specifico, richiede questo tipo di operazioni, al fine di raggiungere un equilibrio tra valori europei e nazionali, che spesso celano scelte di ordine costituzionale e invitano a riflettere, in ultima analisi, sul tipo di società europea in cui desideriamo vivere [310].

[306] Principio 16 del Pilastro europeo dei diritti sociali. Per riferimenti dottrinali, si rinvia a T. HARVEY, *The European Union and the Governance of Health Care*, in G. DE BÚRCA, J. SCOTT (eds.), *Law and New Governance in the EU and the US*, Hart Publishing, London, 2006, p. 202.

[307] Artt. 9, 114, par. 3, 168, par. 1, TFUE nonché art. 35 della Carta. Sul rango particolarmente elevato riconosciuto alla tutela della sanità pubblica nella scala di valori dell'Unione, cfr. sentenze della Corte del 4 maggio 2016, causa C-547/14, *Philip Morris*, ECLI:EU:C:2016:325, punti 153 e 157; del 4 maggio 2016, causa C-477/14, *Pillbox*, ECLI:EU:C:2016:324, punto 116; del 29 aprile 2015, causa C-528/13, *Léger*, ECLI:EU:C:2015:288, punto 57; del 6 settembre 2012, causa C-544/10, *Deutsches Weintor*, EU:C:2012:526, punti 45-47.

[308] Art. 179 TFUE e art. 3, par. 2, TUE.

[309] Si vedano al riguardo le riflessioni svolte da L.S. ROSSI, *op. cit.*, 2024, p. 18.

[310] Per un'analisi di ampio respiro sul concetto di "società europea", si rinvia al contributo di A. VON BOGDANDY, *The Emergence of European Society through Public Law: A Hegelian and Anti-Schmittian Approach*, OUP, Oxford, 2024.

Conclusioni

Il presente lavoro offre un contributo al dibattito dottrinale esistente sullo EHDS, proponendo un'analisi che trae origine dall'osservazione di due dinamiche relative allo sviluppo generale dell'ordinamento giuridico europeo nel campo della tutela della sanità (digitale). La prima dinamica riguarda il crescente ruolo assunto dall'Unione come attore fondamentale nella protezione della salute dei suoi cittadini, soprattutto mediante l'adozione di atti finalizzati al raggiungimento di obiettivi economici e sociali particolarmente ambiziosi. Questo, tuttavia, senza una modifica del diritto primario che rispecchi i maggiori poteri esercitati *de facto* dall'Unione. La seconda, invece, concerne l'impegno sempre maggiore del legislatore europeo nel promuovere la digitalizzazione del settore sanitario non solo utilizzando la leva finanziaria, ma anche adottando nuovi regolamenti come lo EHDS, che favoriscono l'uso e la libera circolazione dei dati, mantenendo un forte ancoraggio alle norme del GDPR così come interpretate dalla Corte.

Partendo da queste osservazioni, sono state identificate due linee di ricerca complementari, ciascuna con un obiettivo distinto ma interconnesse e in un rapporto di continuità. Sul piano sistematico, l'obiettivo è stato migliorare la comprensione dello EHDS nel contesto più ampio del processo di integrazione europea in ambito sanitario. Su quello sostanziale, l'ambizione è stata valutare l'impatto del modello regolatorio introdotto dallo EHDS – e, in generale, dagli atti della Strategia europea per i dati – sulle scelte di bilanciamento operate finora nell'interpretazione e nell'applicazione del GDPR. Per affrontare tali questioni, il lavoro è stato sviluppato in due parti, di cui vale la pena riprendere gli aspetti più salienti.

Nella prima parte, l'analisi del fondamento costituzionale dello EHDS ha permesso di riflettere sull'evoluzione del processo di integrazione nel settore sanitario mettendone in luce due dinamiche tipiche: il ricorso a basi giuridiche "forti" per intervenire in settori dove l'Unione dispone di competenze limitate e la continua aspirazione del legislatore europeo, soprattutto negli ultimi tempi, a coniugare la realizzazione di obiettivi di carattere economico e sociale. Entrambe queste dinamiche sono state analizzate criticamente nel contesto dello EHDS, sia in relazione alla sua conformità con l'attuale quadro costituzionale (capitolo 1) sia rispetto ai rischi di effettività normativa

che possono emergere nella fase di attuazione concreta di tale regolamento (capitolo 2).

In merito al primo profilo, l'analisi ha messo in evidenza come lo EHDS rappresenti un ulteriore esempio di legislazione indiretta, mediante la quale l'Unione persegue obiettivi strategici – come la creazione di un mercato unico digitale e di un'UES – realizzando, di fatto, un'integrazione più profonda nel settore sanitario. In particolare, è stato sottolineato come la forzatura dei limiti costituzionali esistenti, resa possibile anche in ragione dello stretto nesso di funzionalità tra gli obiettivi economici e sociali perseguiti, si realizza utilizzando il "grimaldello" della protezione/libera circolazione dei dati personali e non più solo del mercato interno. L'art. 16, par. 2, TFUE va, quindi, ad arricchire la c.d. "*web of competence*" [1], ampliando la portata e l'incisività dell'azione dell'Unione in un numero di settori potenzialmente illimitato, dal momento che, alla luce del processo di digitalizzazione, sarà sempre più difficile pensare a un qualsivoglia ambito che non presenti un (seppur labile) collegamento con la protezione/libera circolazione dei dati personali.

Quanto ai rischi di effettività, l'esame svolto nel capitolo 2 ha messo in luce due fattori che potrebbero compromettere la realizzazione degli obiettivi economici e sociali dello EHDS. Il primo riguarda l'assenza e l'insufficiente coordinamento tra lo EHDS e altri atti di diritto derivato (*in primis*, il GDPR, ma anche il MDR e l'AIA) che solleva questioni non solo sostanziali, ma anche istituzionali, in merito al ruolo e al coordinamento tra le diverse autorità competenti. Sebbene siano stati solo parzialmente trattati in questa sede, tali aspetti meritano di essere ulteriormente indagati, specialmente per chiarire la ripartizione delle competenze e le modalità con cui si concretizzano gli obblighi di leale cooperazione tra autorità nazionali [2], come quelle designate dallo EHDS e quelle di controllo previste dal GDPR [3]. Il secondo fattore critico concerne le scelte di bilanciamento tra diritti e interessi potenzialmente confliggenti nell'interpretazione e applicazione dello EHDS. A quest'ultimo proposito, è stato sottolineato che la possibilità di raggiungere gli obiettivi

---

[1] K.P. PURNHAGEN et al., *More Competences than You Knew?: The Web of Health Competence for European Union Action in Response to the COVID-19 Outbreak*, in *Eur. J. Risk Regul*., 2020, vol. 11, n. 2, p. 297.

[2] Sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms e a*., ECLI:EU:C:2023:537, punto 52. Principio affermato dalla Corte anche nell'ambito del meccanismo dello sportello unico previsto dagli artt. 60-65 del GDPR nella sentenza del 15 giugno 2021, causa C-645/19, *Facebook Ireland e a*., ECLI:EU:C:2021:483, punti 63-64, e poi nella sentenza del 29 gennaio 2025, cause riunite T-70/23, T-84/23 e T-111/23, *Data Protection Commission c. EDPB*, ECLI:EU:T:2025:116, punto 53.

[3] Un tentativo, seppur preliminare, di sistematizzazione è stato proposto altrove: cfr. A. FIORENTINI, *Rethinking the Institutional Framework for the EU Data Regulations: Towards an Enhanced Administrative Integration*, in *REALaw*, 2025, vol. 18, n. 3, pp. 51-79.

prefissati dipenderà dall'attenzione prestata dall'interprete non solo al rapporto di funzionalità tra gli obiettivi economici e sociali dello EHDS, ma anche alla dimensione individuale e collettiva dei diritti coinvolti, in particolare del diritto alla salute e alla protezione dei dati personali.

La seconda parte si è concentrata proprio su quest'ultimo aspetto, approfondendo il rapporto tra il diritto degli individui a esercitare il controllo sui propri dati e l'interesse, tanto di soggetti terzi quanto della collettività, al loro utilizzo. Il passaggio dalla prima alla seconda parte non è stato dunque meramente sequenziale, ma concettualmente necessario: solo mettendo a fuoco la stretta interrelazione tra le finalità economiche e sociali – esplicite e implicite – dello EHDS, infatti, è stato possibile cogliere appieno la portata delle scelte di bilanciamento che il regolamento propone e le loro implicazioni in materia di protezione di dati personali. Quest'ultima non viene più concepita esclusivamente come un limite all'utilizzo dei dati, ma come componente integrante di una governance orientata a valorizzarne la funzione sociale.

Sulla base di queste considerazioni, l'analisi svolta nei capitoli 3 e 4 ha evidenziato un aspetto piuttosto rilevante. Nonostante la sostanziale coincidenza dell'approccio regolatorio utilizzato dal legislatore europeo nello EHDS e nel GDPR per giungere a un equilibrio tra i diversi diritti e interessi in gioco, è possibile che tra le due discipline sorgano tensioni costituzionali e fisiologiche, soprattutto se si considera il modo in cui il GDPR è stato finora interpretato e applicato. A questo proposito, per evitare che le suddette tensioni possano compromettere la realizzazione degli obiettivi non solo dello EHDS, ma anche dello stesso GDPR, sono state proposte alcune strategie interpretative e legislative che mirano a un'interpretazione (capitolo 3) e un'applicazione (capitolo 4) del GDPR maggiormente in linea con le novità introdotte dallo EHDS e, più in generale, dagli atti della Strategia europea per i dati.

A tale fine, nel capitolo 3, dopo aver illustrato le garanzie introdotte dallo EHDS per evitare che l'uso e la condivisione dei dati sanitari elettronici compromettano le tutele previste per gli interessati, è stata proposta un'interpretazione del GDPR che rispecchi i suoi "veri" obiettivi. In particolare, è emerso un aspetto cruciale che vale la pena ribadire: l'individuazione di alternative ermeneutiche riguardo al campo di applicazione materiale del GDPR è almeno in parte ostacolata dall'uso di termini generici nelle definizioni di concetti chiave della disciplina come "trattamento" e "dati personali"; d'altro canto maggiori margini di manovra si hanno con riferimento alle norme del GDPR che consentono di bilanciare il diritto alla protezione dei dati personali con altri diritti e libertà fondamentali. Rispetto a queste ultime, è stata sottolineata l'importanza di evitare automatismi nelle operazioni di bilanciamento che portano al prevalere del diritto individuale alla protezione dei dati personali *by default*, privilegiando invece un approccio che valuti concretamente i diritti e gli interessi in gioco e applichi in modo sistematico il principio di proporzionalità.

Nel capitolo 4, infine, sono state elaborate proposte di revisione del quadro normativo esistente sulla base dell'analisi comparativa della normativa italiana e francese di applicazione delle disposizioni del GDPR sul trattamento dei dati sanitari per fini di ricerca scientifica, nonché delle prassi amministrative delle rispettive autorità di controllo. In primo luogo, sono state ipotizzate modifiche del GDPR che, tra le altre cose, consentono di stabilire una soglia minima di bilanciamento *ex lege* al fine di sistematizzare i diritti e gli interessi in gioco, da integrare con un bilanciamento *ex post*. In secondo luogo, considerando la scarsa probabilità di una revisione complessiva del GDPR, è stata approfondita una possibile strategia alternativa: quella di sottoporre le normative nazionali più problematiche, per quanto riguarda la realizzazione dell'obiettivo della libera circolazione dei dati, al vaglio della Corte, affinché ne valuti la compatibilità con il GDPR. L'auspicio è che, in questi casi, l'interpretazione offerta sia il frutto di una ponderazione dei diritti e degli interessi in gioco che tenga conto degli effetti positivi per la collettività derivanti dall'uso e dalla condivisione dei dati nell'Unione, permettendo così di avviare un processo di riforma a livello nazionale.

Alla luce degli approfondimenti sopra riassunti, ritengo utile avanzare alcune possibili risposte alle domande sollevate nella parte introduttiva del lavoro. Innanzitutto, per quanto riguarda la questione di carattere sistematico relativa al modo in cui lo EHDS si inserisce nel più ampio processo di integrazione europea in ambito sanitario, è emerso che tale regolamento si pone in perfetta continuità rispetto alle dinamiche tipiche di questo processo. L'unico aspetto di novità individuato rispetto al passato concerne l'art. 16, par. 2, TFUE che rappresenta per l'Unione un ulteriore strumento per forzare le strette maglie dell'attuale assetto di competenze. A questo proposito, non posso esimermi dal sottolineare come l'esistenza di una "*web of competence*" sempre più estesa rischi di rendere strutturale la "*competence creep*", trasformandola da "problema" da risolvere a un *modus operandi* dell'Unione, che lungi dall'essere circoscritto al solo ambito sanitario, investe ormai una pluralità di settori strategici, tra cui l'industria, la protezione civile e la sicurezza [4].

[4] Si vedano, tra gli altri, P. DE PASQUALE, *Dalla flessibilità delle basi giuridiche alla normazione integrata: tecniche legislative funzionali alla rigidità del riparto di competenze nell'UE*, in *DUE*, 2025, vol. 1, p. 3 ss.; F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revised*, in *Eur. Foreign Aff. Rev.*, 2023, vol. 28, n. 4, pp. 323-340; C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO, *La trasformazione digitale in Europa. Diritti e principi*, Giappichelli, Torino, 2023, p. 9 ss.; F. CASOLARI, *The EU Approach towards Disaster Management. A Critical Appraisal in the Light of the Action Put in Place to Face the COVID-19 Pandemic*, in *YIDL*, 2023, vol. 4, n. 1, p. 53; B. DE WITTE, *The European Union's COVID-*

In questo scenario, il principio di attribuzione rischia di perdere il suo ruolo di "principio fondante" dell'ordinamento giuridico europeo, lasciando che a orientare l'azione dell'Unione non siano più i limiti costituzionali, bensì la volontà politica di realizzare determinati obiettivi. Di fronte alla decisione di elevare la trasformazione digitale, non solo in ambito sanitario, a una delle principali priorità dell'Unione e, per scelta o per riflesso, degli Stati membri, ci si potrebbe chiedere se abbia ancora senso vigilare sul rispetto della delimitazione delle competenze tra Unione e Stati membri. Nella pratica, la risposta sembra essere negativa. Presupponendo, infatti, un livello di armonizzazione difficilmente realizzabile dai singoli Stati membri, il processo di digitalizzazione rende problematico preservare le specificità nazionali, che dovrebbero riflettere i diversi equilibri politico-sociali, specialmente se sono gli stessi Stati a non difenderle.

Tale constatazione può trovare un fondamento argomentativo nella giurisprudenza consolidata della Corte, la quale, richiamandosi al principio di leale cooperazione di cui all'art. 4, par. 3, TUE, ha escluso che gli Stati membri possano invocare prerogative sovrane per sottrarsi unilateralmente agli obblighi previsti dai Trattati [5]. Su questa base si è affermata la c.d. "teoria della limitazione", che, applicandosi ormai in maniera trasversale a settori eterogeni (ad es. l'organizzazione del sistema giudiziario [6] o i criteri di attribuzione della cittadinanza [7]), riduce progressivamente lo spazio di autonomia nazionale in nome del perseguimento degli obiettivi dell'Unione [8], fino al punto da indurre a ritenere che "*[t]here simply is no nucleus of sovereignty that the Member States can invoke, as such, against the Community*" [9].

Eppure, come osserva Weiler, in una realtà federale come quella europea il rispetto dei confini di competenza e delle procedure decisionali è importante

---

19 Recovery Plan: The Legal Engineering of an Economic Policy Shift, in *CML Rev*., 2021, vol. 58, pp. 635-682; G. DI FEDERICO, *Principio di attribuzione e competenze esclusive degli Stati tra mito e realtà* (in corso di pubblicazione).

[5] V., *inter alia*, sentenza della Corte, 10 dicembre 1969, cause riunite C-6/69 e C-11/69, *Commissione c. Francia*, ECLI:EU:C:1969:68, punti 14-15.

[6] Sentenza della Corte del 5 novembre 2019, causa C-192/18, *Commissione c. Polonia*, ECLI:EU:C:2019:924.

[7] Sentenza della Corte del 29 aprile 2025, causa C-181/23, *Commissione c. Malta*, ECLI:EU:C:2025:283.

[8] Per una disamina delle principali sentenze della Corte che hanno definito i tratti essenziali della suddetta teoria, cfr. F. CASOLARI, *La tutela dei valori dell'Unione europea e le prerogative sovrane degli Stati membri: quali limitazioni?*, in *Unione europea e diritti*, 2025, n. 3, pp. 1-17.

[9] K. LENAERTS, *Constitutionalism and the Many Faces of Federalism*, in *The American Journal of Comparative Law*, 1990, vol. 38, n. 2, p. 220.

quanto la tutela dei diritti fondamentali [10]. Per questo, pur riconoscendo la prassi sopra descritta – che, come stabilito dalla Corte, non può comunque giustificare l'inosservanza del diritto primario [11] –, la risposta alla domanda se abbia senso vigilare sulla delimitazione delle competenze non può che essere positiva. Fintanto che non si decida unanimemente di modificare i principi che regolano l'esistenza e l'esercizio delle competenze dell'Unione quale Unione di diritto, la strada da percorrere dovrebbe essere quella di una modifica dei Trattati che dia formale riconoscimento ai maggiori poteri che l'Unione già esercita. Per quanto riguarda il settore sanitario, le opzioni possibili spaziano da un trasferimento integrale della materia a livello sovranazionale a una più realistica [12] estensione dell'elenco di ambiti contenuti all'art. 168, par. 4, TFUE [13].

Una simile modifica permetterebbe, in primo luogo, di garantire una maggiore legittimità democratica dell'azione dell'Unione, evitando che il legislatore europeo si sostituisca al legislatore nazionale, privandolo o limitandone l'autonomia prevista dai Trattati, senza che gli Stati membri abbiano esplicitamente acconsentito a tale trasferimento di competenze [14]. In secondo luogo, assicurerebbe un maggior livello di trasparenza, *accountability* e intelligibilità per i cittadini europei [15], evitando, ad esempio, che atti aventi come fine principale la tutela della salute vengano adottati "*under a false label, as if they are all about promoting trade, making more of it and removing obstacles in a*

---

[10] J.H.H. WEILER, *Vendesi cittadinanza. Commissione c. Malta: chi, davvero, smercia i valori europei*, in *QC*, 2024, vol. XLIV, n. 2, p. 458.

[11] Sentenza della Corte del 9 dicembre 1997, causa C-265/95, *Commissione c. Francia*, ECLI:EU:C:1997:595, punti 55-56.

[12] Come noto, la procedura di revisione ordinaria prevista dall'art. 48, parr. 2-5, TUE richiede il raggiungimento dell'unanimità tra gli Stati membri, nonché la ratifica del nuovo Trattato da parte degli stessi ("doppia unanimità"). Per un commento all'art. 48 TFUE, v. KLAMERT M., *Article 48*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *The EU Treaties and the Charter of Fundamental Rights. A Commentary*, Oxford University Press, Oxford, 2019, p. 302 ss.

[13] Stabilendo gli ambiti per cui il legislatore europeo è legittimato a ricorrere a misure di armonizzazione in materia di sanità pubblica, una modifica del quarto paragrafo dell'art. 168 TFUE permetterebbe di assicurare all'Unione uno spazio di intervento piuttosto ampio, vista la prospettiva di una sempre maggiore digitalizzazione della sanità, senza tuttavia sottrarre alla competenza degli Stati membri l'intera materia.

[14] M. DOUGAN, *Legal Developments*, in *JCMS*, 2010, vol. 48, pp. 163-181. Si veda anche S. GARBEN, *Competence Creep Revised*, in *J. Common Mark. Stud*., 2019, vol. 57, n. 2, p. 215 ss., che tuttavia sottolinea come la "*indirect legislation*" è la forma di integrazione meno problematica dal punto di vista della legittimità democratica dell'azione dell'Unione, rispetto alla "*negative integration through case-law*" e alla "*parallel integration*".

[15] *È.* BULAND, A. FIORENTINI, *The Day After the CoFoE (Act II): The EU Treaty Revision at the Mercy of Enlargement?*, in *Quaderni AISDUE*, 2024, fasc. 1, p. 286.

concrete, narrow, sense" [16]. In terzo luogo, sapere che l'Unione può intervenire in modo incisivo in un certo settore potrebbe stimolare i diversi portatori di interesse e i Parlamenti nazionali a essere maggiormente attivi nell'influenzare il processo decisionale non solo a livello nazionale, ma anche a livello europeo [17].

Eventualmente, qualora non si trovasse un accordo sulla possibilità di trasferire (*in toto* o parzialmente) la materia in questione all'Unione, potrebbe essere sensato perlomeno ipotizzare di percorrere strade che consentano di garantire una maggiore legittimazione democratica delle decisioni sovranazionali. A quest'ultimo proposito, ad esempio, si potrebbe considerare l'opportunità di rafforzare il controllo *ex ante* dei Parlamenti nazionali, estendendo il termine per la presentazione dei pareri sul rispetto della sussidiarietà [18] e ampliando la gamma di contestazioni possibili (ad es. sul rispetto del principio di proporzionalità e dell'identità nazionale) [19]. Inoltre, per fare in modo che le decisioni in ambito sanitario siano prese da attori istituzionali dotati di una profonda comprensione delle questioni sostanziali e dei diritti

---

[16] G. DAVIES, *The Competence to Create an Internal Market: Conceptual Poverty and Unbalanced Interests*, in S. GARBEN, I. GOVAERE (eds.), *The Division of Competences Between the EU and the Member States: Reflections on the Past, the Present and the Future*, Hart Publishing, Oxford, 2017, pp. 74-89.

[17] S. GARBEN, *Confronting the Competence Conundrum: Democratising the European Union through an Expansion of Its Legislative Powers*, in *Oxf. J. Leg. Stud.*, 2015, vol. 35, n. 1, p. 79. Similmente, con riferimento specifico al settore sanitario, M. MCKEE, A. DE RUIJTER, *The Path to a European Health Union*, in *The Lancet Regional Health – Europe*, 2024, vol. 36, p. 3, confidano sull'assunto che un maggiore potere dell'Unione porterà a un rafforzamento del coinvolgimento del livello nazionale (ad es. dipartimenti sanitari e relativo know-how della comunità professionale) nel processo politico dell'Unione in ambito sanitario.

[18] Ad esempio, la Risoluzione sui progetti del Parlamento europeo intesi a modificare i Trattati (2022/2051(INL)), del 22 novembre 2023 estende a 12 settimane il termine per la procedura del "cartellino giallo". Inoltre, viene previsto che la Commissione tenga conto dei pareri motivati dei parlamenti nazionali e dei parlamenti regionali con poteri legislativi nelle sue relazioni annuali sui principi di sussidiarietà e di proporzionalità. In aggiunta, dovrebbe anche mettere a disposizione del Consiglio e del Parlamento le informazioni sulle obiezioni nel corso della procedura legislativa, qualora i parlamenti nazionali presentassero "un numero significativo" di pareri motivati su un determinato progetto legislativo (emendamento 221).

[19] Inoltre, si potrebbe decidere di attribuire ai Parlamenti nazionali che presentano pareri motivati alle istituzioni dell'Unione (e ai comitati consultati nella fase iniziale della procedura legislativa) la facoltà di esprimere – entro un termine stabilito – un parere contrario all'adozione di un certo atto. Questo parere dovrebbe essere tenuto in considerazione nel caso in cui gli Stati membri decidano di presentare un ricorso per annullamento *ex* art. 263 TFUE. A questo proposito, sarebbe opportuno che il termine di 2 mesi previsto dall'art. 263 TFUE venisse esteso, in modo da assicurare agli Stati membri una finestra di tempo più ampia per valutare in concreto gli effetti di un atto in termini di rispetto dei principi di sussidiarietà e di proporzionalità.

fondamentali relativi alla tutela della salute, oltre che consapevoli delle specificità di tale settore [20], si dovrebbe prendere in seria considerazione l'istituzione di una configurazione *ad hoc* sia nel Consiglio sia nel Parlamento [21]. Queste riforme istituzionali non richiedono una modifica del Trattato, ma piuttosto una decisione presa, rispettivamente, dal Consiglio europeo a maggioranza qualificata [22] e dalla Conferenza dei presidenti del Parlamento [23].

Con riferimento alla seconda domanda di carattere sostanziale sull'esistenza di possibili tensioni costituzionali e fisiologiche tra i modelli regolatori adottati per lo EHDS e il GDPR, i risultati raggiunti suggeriscono che vi sia, almeno a livello teorico, una sostanziale continuità tra le scelte compiute dal legislatore nell'adozione di queste due normative. Tuttavia, viste le frizioni che possono emergere se si considera il modo in cui il GDPR è stato interpretato e attuato, ritengo che i tempi siano maturi affinché i delicati equilibri costituzionali tra i diritti degli individui e gli interessi della collettività, già *in nuce* nel GDPR, si realizzino pienamente. Anche alla luce di alcune considerazioni svolte nella prima parte del presente lavoro emerge chiaramente la volontà legislativa – maturata in particolare a seguito della pandemia da Covid-19 – di evitare che la barriera eretta a tutela dell'individuo e delle sue libertà pregiudichi interessi fondamentali della società (ad es. la protezione della sanità pubblica, la sostenibilità ambientale, la lotta contro il terrorismo e la prevenzione dei reati).

Dalla lettura dello EHDS, così come degli altri regolamenti sui dati adottati nell'ambito della Strategia del 2020 emerge in modo evidente una matrice solidaristica [24], che ha permesso di trovare un ragionevole punto di saldatura

---

[20] T. HERVEY, A. DE RUIJTER, *op. cit*., 2020, pp. 733-734.

[21] Con riferimento al Parlamento, ad esempio, si è deciso di formalizzare la scissione della Commissione parlamentare per l'ambiente, la sanità pubblica e la sicurezza alimentare (ENVI), assicurando all'attuale sottocommissione per la salute pubblica (SANT) lo status di commissione permanente. Cfr. https://www.europarl.europa.eu/news/en/press-room/20241218IPR26022/sant-parliament-confirms-standing-committee-for-public-health?xtor=AD-78-[Social_share_buttons]-[linkedin]-[en]-[news]-[pressroom]-[sant-chair-statement-on-establishing-standing]&.

[22] Artt. 16, par. 6, TUE e 236 TFUE.

[23] Art. 27, par. 7, Regolamento del Parlamento europeo.

[24] Si consideri, ad esempio, il DGA che, al capo IV, disciplina il meccanismo dell'altruismo dei dati, ossia la condivisione volontaria di dati subordinata al consenso dell'interessato (nel caso di dati personali) o all'autorizzazione del titolare (nel caso di dati non personali) finalizzato al perseguimento di obiettivi di interesse generale. Il DGA prevede anche la facoltà *ex* art. 3 per gli enti pubblici di mettere a disposizione determinati dati (ad es. quelli protetti per motivi di riservatezza commerciale) da loro detenuti in modo da consentirne il riutilizzo sulla base di specifiche condizioni (art. 5 DGA). La medesima facoltà di condivisione è prevista *ex* art. 16 per le organizzazioni per l'altruismo dei dati per motivi di interesse generale. Accanto a queste forme di solidarietà volontaria, i regolamenti della Strategia europea dei dati,

tra la tutela del singolo e gli interessi della collettività, riconoscendo che la realizzazione dell'uno non comporta necessariamente l'annullamento dell'altro. Questi sviluppi normativi – frutto di scelte di ordine costituzionale che, senza inficiare le tutele per l'individuo, riconoscono l'esigenza della società di sfruttare il potenziale dei dati, specialmente in settori come quello sanitario, dove dal loro uso e condivisione derivano importanti effetti positivi per la collettività – gettano nuova luce sul modo in cui la disciplina sulla protezione e libera circolazione dei dati personali è stata interpretata e attuata finora.

L'interprete di tale disciplina, così come dei regolamenti sui dati della Strategia, deve necessariamente tener conto del mutato contesto socioculturale e normativo, caratterizzato da una crescente consapevolezza della necessità di limitare il diritto individuale alla protezione dei dati personali per dare attuazione a diritti fondamentali e principi generali, come il diritto alla salute [25] e i principi di non discriminazione e di equo accesso a cure sanitarie di qualità [26], nonché di contribuire alla realizzazione di obiettivi quali la tutela della sanità pubblica [27], della ricerca e del progresso scientifico e tecnologico [28]. Di conseguenza, invece di interpretare queste normative riaffermando l'assoluta centralità della persona e delle sue prerogative, è bene che venga riconosciuta maggiormente la dimensione collettiva della protezione dei dati personali.

In definitiva, un'interpretazione e applicazione del GDPR basata su una valutazione sistemica ed equilibrata degli obiettivi di tale regolamento e delle novità introdotte dai regolamenti della Strategia europea dei dati garantirà una

---

in particolare lo EHDS e il DA, contemplano ulteriori modalità di condivisione dei dati basate su obblighi normativi e dunque riconducibili a una forma di "solidarietà imposta". Nello EHDS, ad esempio, l'art. 5 introduce un obbligo per gli Stati membri di mettere a disposizione determinate categorie di dati sanitari elettronici per l'uso primario; mentre l'art. 51 impone ai titolari di condividere alcune categorie di dati elettronici, tra cui le cartelle cliniche elettroniche, per l'uso secondario. Similmente, il DA prescrive obblighi di condivisione dei dati generati da prodotti o servizi correlati sia tra imprese (B2B) che tra imprese e consumatori (B2C) (capo II), oltre a prevedere, in situazioni eccezionali come le emergenze sanitarie, la condivisione tra imprese ed enti pubblici (B2G) (capo V). Si vedano anche le osservazioni svolte nella sezione 2.1 del capitolo 2. In dottrina, alcuni autori hanno già prospettato l'esistenza di un vero e proprio principio normativo di solidarietà nell'ambito della protezione dei dati personali. Si vedano, in particolare, i contributi di: F. BRAVO, *Il principio di solidarietà*, in F. BRAVO (a cura di), *Dati personali, protezione, libera circolazione e governance. I principi*, Pacini Giuridica, Pisa, 2023, p. 541 ss.; ID., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, vol. 2, p. 405 ss; ID., *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf.*, 2023, vol. 3, p. 481 ss.

[25] Art. 35 della Carta.

[26] Principio 16 del Pilastro europeo dei diritti sociali.

[27] Artt. 9, 114, par. 3, 168, par. 1, TFUE nonché art. 35 della Carta.

[28] Art. 179 TFUE e art. 3, par. 2, TUE.

maggiore coerenza nell'ordinamento giuridico dell'Unione. Questo diverso approccio permetterà anche di contribuire alla ricostruzione delle fondamenta concettuali della disciplina della protezione dei dati personali e del diritto fondamentale sancito dall'art. 8 della Carta [29], in grado di riflettere più fedelmente gli attuali equilibri costituzionali in materia di dati personali. Sarà così possibile superare l'apparente inconciliabilità tra il diritto del singolo a un controllo sempre più attento e capillare dei dati personali che lo riguardano e l'interesse della collettività all'uso di tali dati per finalità di interesse generale.

[29] Come sottolineato a più riprese nel presente lavoro (v., in particolare, la sezione 4.2 del capitolo 2 e la sezione 3.2 del capitolo 3), la prima va intesa come normativa volta, da un lato, a proteggere i diritti e le libertà delle persone fisiche dai danni derivanti dal trattamento dei dati personali e, dall'altro, a riconoscere l'importanza che attività di trattamento legittime rivestono per la società moderna. Il secondo, invece, va ricostruito come diritto ad avere "*a (set of) rule(s) regulating the processing of personal data*" (cfr. L. DALLA CORTE, *A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection*, in D. HALLINAN et al. (eds.), *Data Protection and Privacy: Data Protection and Democracy*, Hart Publishing, Oxford, 2020, pp. 27-58) o, per usare le parole della Corte, come "diritto ad un trattamento lecito dei loro dati personali" (sentenza *Quirin Privatbank*, punto 40).

Bibliografia

LEGISLAZIONE

Legislazione europea

Decisioni

Decisione della Commissione del 16 settembre 2021 che istituisce l'autorità per la preparazione e la risposta alle emergenze sanitarie, C/2021/6712, final.

Decisione (UE) 2019/420 del Parlamento europeo e del Consiglio del 13 marzo 2019 che modifica la decisione n. 1313/2013/UE su un meccanismo unionale di protezione civile, *GU L 77I del 20.3.2019, pp. 1-15.*

Decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio del 22 ottobre 2013 relativa alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 2119/98/CE, *GU L 293 del 5.11.2013, pp. 1-15.*

Decisione di esecuzione (UE) 2019/1269 della Commissione del 26 luglio 2019 che modifica la decisione di esecuzione 2014/287/UE della Commissione che stabilisce criteri per l'istituzione e la valutazione delle reti di riferimento europee e dei loro membri e per agevolare lo scambio di informazioni e competenze in relazione all'istituzione e alla valutazione di tali reti, *GU L 200 del 29.7.2019, pp. 35-43.*

Decisione di esecuzione della Commissione del 22 dicembre 2011 che stabilisce le norme per l'istituzione, la gestione e il funzionamento della rete di autorità nazionali responsabili dell'assistenza sanitaria on line, *GU L 344 del 28.12.2011, pp. 48-50.*

Decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, *GU L 350 del 30.12.2008, pp. 60-71.*

Direttive

Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione), *GU L 172 del 26.6.2019, pp. 56-83.*

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, pp. 89-131.*

Direttiva 2011/24/UE del Parlamento europeo e del Consiglio del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, *GU L 88 del 4.4.2011, pp. 45-65.*

Direttiva 2006/123/CE del Parlamento europeo e del Consiglio del 12 dicembre 2006 relativa ai servizi nel mercato interno, *GU L 376 del 27.12.2006, pp. 36-68.*

Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003 relativa al riutilizzo dell'informazione del settore pubblico, *GU L 345 del 31.12.2003, pp. 90-96.*

Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico"), *GU L 178 del 17.7.2000, pp. 1-16.*

Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, *GU L 77 del 27.3.1996, pp. 20-28.*

Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, *GU L 281 del 23.11.1995, pp. 31-50.*

Direttiva 82/501/CEE del Consiglio del 24 giugno 1982 sui rischi di incidenti rilevanti connessi con determinate attività industriali, *GU L 230 del 5.8.1982, pp. 1-18.*

Direttiva 65/65/CEE del Consiglio del 26 gennaio 1965 per il ravvicinamento delle disposizioni legislative, regolamentari e amministrative relative alle specialità medicinali, *GU 22 del 9.2.1965, pp. 369-373.*

Regolamenti

Regolamento (UE) 2025/2518 del Parlamento europeo e del Consiglio, del 26 novembre 2025, che stabilisce norme procedurali aggiuntive sull'applicazione del regolamento (UE) 2016/679, *GU L, 2025/2518, 12.12.2025*.

Regolamento delegato (UE) 2025/2050 della Commissione, del 10 luglio 2025 che integra il regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio stabilendo le condizioni tecniche e le procedure alle quali i fornitori di piattaforme online di dimensioni molto grandi e di motori di ricerca online di dimensioni molto grandi devono condividere i dati con ricercatori abilitati, *GU L, 2025/2050, 9.10.2025*.

Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847, *GU L, 2025/327, 5.3.2025.*

Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828, *GU L, 2024/2847, 20.11.2024*.

Regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio, del 13 giugno 2024, sui parametri di qualità e sicurezza per le sostanze di origine umana destinate all'applicazione sugli esseri umani e che abroga le direttive 2002/98/CE e 2004/23/CE, *GU L, 2024/1938, 17.7.2024.*

Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), *GU L, 2024/1689, 12.7.2024*.

Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024

che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale, *GU L, 2024/1183, 30.4.2024.*

Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati), *GU L, 2023/2854, 22.12.2023.*

Regolamento (UE) 2023/1781 del Parlamento europeo e del Consiglio del 13 settembre 2023 che istituisce un quadro di misure per rafforzare l'ecosistema europeo dei semiconduttori e che modifica il regolamento (UE) 2021/694 (regolamento sui chip), *GU L 229 del 18.9.2023, pp. 1-53.*

Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio del 23 novembre 2022 relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE, *GU L 314 del 6.12.2022, pp. 26-63.*

Regolamento (UE) 2022/2370 del Parlamento europeo e del Consiglio del 23 novembre 2022 recante modifica del regolamento (CE) 851/2004, con il quale si crea un Centro europeo per la prevenzione e il controllo delle malattie, *GU L 314 del 6.12.2022, pp. 1-25.*

Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), *GU L 277 del 27.10.2022, pp. 1-102.*

Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), *GU L 265 del 12.10.2022, pp. 1-66.*

Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati), *GU L 152 del 3.6.2022, pp. 1-44*.

Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici, *GU L 20 del 31.1.2022, pp. 1-37.*

Regolamento (UE) 2021/2282 del Parlamento europeo e del Consiglio del 15 dicembre 2021 relativo alla valutazione delle tecnologie sanitarie e che modifica la direttiva 2011/24/UE, *GU L 458 del 22.12.2021, pp. 1-32.*

Regolamento (UE) 2021/1153 del Parlamento europeo e del Consiglio del 7 luglio 2021 che istituisce il meccanismo per collegare l'Europa e abroga i regolamenti (UE) n. 1316/2013 e (UE) n. 283/2014, *GU L 249 del 14.7.2021, pp. 38-81*.

Regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio del 14 giugno 2021 su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla COVID-19 (certificato COVID digitale dell'UE) per agevolare la libera circolazione delle persone durante la pandemia di COVID-19, *GU L 211 del 15.6.2021, pp. 1-2*.

Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240, *GU L 166 dell'11.05.2021, pp. 1-34.*

Regolamento (UE) 2021/695 del Parlamento europeo e del Consiglio del 28 aprile 2021 che istituisce il programma quadro di ricerca e innovazione Orizzonte Europa e ne

stabilisce le norme di partecipazione e diffusione, e che abroga i regolamenti (UE) n. 1290/2013 e (UE) n. 1291/2013, *GU L 170 del 12.5.2021, pp. 1-68.*

Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio del 24 marzo 2021 che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 ("programma UE per la salute") (EU4Health) e che abroga il regolamento (UE) n. 282/2014, *GU L 107 del 26.3.2021, pp. 1-29.*

Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, *GU L 57 del 18.2.2021, pp. 17-75.*

Regolamento (UE) 2020/2094 del Consiglio del 14 dicembre 2020 che istituisce uno strumento dell'Unione europea per la ripresa, a sostegno della ripresa dell'economia dopo la crisi COVID-19, *GU L 433I del 22.12.2020, pp. 23-27*.

Regolamento (UE) 2019/788 del Parlamento europeo e del Consiglio del 17 aprile 2019 riguardante l'iniziativa dei cittadini europei, *GU L 130 del 17.5.2019, pp. 55-81.*

Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, *GU L 303 del 28.11.2018, pp. 59-68.*

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 del 21.11.2018, pp. 39-98.*

Regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012, *GU L 295 del 21.11.2018, pp. 1-38*.

Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio, *GU L 117 del 5.5.2017, pp. 1-175.*

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), *GU L 119 del 4.5.2016, pp. 1-88.*

Regolamento (UE) 536/2014 del Parlamento europeo e del Consiglio del 16 aprile 2014 sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE, *GU L 158 del 27.5.2014, pp. 1-76.*

Regolamento (UE) 182/2011 del Parlamento europeo e del Consiglio del 16 febbraio 2011 che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione, *GU L 55 del 28.2.2011, pp. 13-18.*

Regolamento (CE) 864/2007 del Parlamento europeo e del Consiglio, dell'11 luglio 2007, sulla legge applicabile alle obbligazioni extracontrattuali (Roma II), *GU L 199 del 31.7.2007, pp. 40-49.*

Regolamento (CE) 851/2004 del Parlamento Europeo e del Consiglio del 21 aprile 2004 con il quale si crea un Centro europeo per la prevenzione e il controllo delle malattie, *GU L 142 del 30.4.2004, pp. 1-11.*

Regolamento (CE) 999/2001 del Parlamento europeo e del Consiglio del 22 maggio 2001 recante disposizioni per la prevenzione, il controllo e l'eradicazione di alcune encefalopatie spongiformi trasmissibili, *GU L 147 del 31.5.2001, pp. 1-40.*

Soft law

Accordo interistituzionale "Legiferare meglio" tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea, *GU L 123 del 12.5.2016, pp. 1-14.*

Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia europea per le infrastrutture di ricerca e tecnologia, COM(2025) 497 final, del 15 settembre 2025.

–, Bussola per la competitività dell'UE, COM(2025) 30 final, del 29 gennaio 2025.

Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, L'Unione europea della salute: agire insieme per la salute delle persone, COM(2024) 206 final, del 22 maggio 2024.

–, Aggiornamento della nuova strategia industriale 2020: costruire un mercato unico più forte per la ripresa dell'Europa, COM(2021) 350 final, del 5 maggio 2021.

–, Legiferare meglio: unire le forze per produrre leggi migliori, COM(2021) 219 final, del 29 aprile 2021.

–, Bussola per il digitale 2030: il modello europeo per il decennio digitale, COM(2021) 118 final, del 9 marzo 2021.

–, Comunicazione della Commissione al Parlamento europeo e al Consiglio, Piano europeo di lotta contro il cancro, COM(2021) 44 final, del 3 febbraio 2021.

–, Strategia per rafforzare l'applicazione della Carta dei diritti fondamentali dell'Unione europea, COM(2020) 711 final, del 2 dicembre 2020.

–, Strategia farmaceutica per l'Europa, COM(2020) 761 final, del 25 novembre 2020.

–, Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE alle minacce per la salute a carattere transfrontaliero, COM(2020) 724 final, dell'11 novembre 2020.

–, Un nuovo SER per la ricerca e l'innovazione, COM(2020) 628 final, del 30 settembre 2020.

–, Attuazione delle corsie verdi ("*green lanes*") previste dagli orientamenti relativi alle misure per la gestione delle frontiere destinate a tutelare la salute e garantire la disponibilità di beni e servizi essenziali (2020/C 96 I/01), del 23 marzo 2020.

–, Individuare e affrontare le barriere al mercato unico, COM (2020) 93 final, del 10 marzo 2020.

–, Plasmare il futuro digitale dell'Europa, COM(2020) 67 final, del 19 febbraio 2020.

–, Una strategia europea per i dati, COM(2020) 66 final, del 19 febbraio 2020.

– *Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union*, COM(2019) 250 final, del 29 maggio 2019.

–, Trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana, COM(2018) 233 final, del 25 aprile 2018.

–, Revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, COM(2017) 228 final, del 10 maggio 2017.

–, Strategia per il mercato unico digitale in Europa, COM(2015) 192 final, del 6 maggio 2015.

–, Piano d'azione Sanità elettronica 2012-2020. Una sanità innovativa per il 21esimo secolo, COM(2012) 736 final, del 6 dicembre 2012.
–, L'Atto per il mercato unico II. Insieme per una nuova crescita, COM(2012) 573 final, del 3 ottobre 2012.
–, Un partenariato rafforzato per lo spazio europeo della ricerca a favore dell'eccellenza e della crescita, COM(2012) 392 final, del 17 luglio 2012.
–, Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo, COM(2012) 9 final, del 25 gennaio 2012.
–, Un quadro coerente per rafforzare la fiducia nel mercato unico digitale del commercio elettronico e dei servizi online, COM(2011) 942 final, dell'1 novembre 2011.
–, Verso un atto per il mercato unico. Per un'economia sociale di mercato altamente competitiva: 50 proposte per lavorare, intraprendere e commerciare insieme in modo più adeguato, COM(2010) 608 final, del 27 ottobre 2010.
–, Un'agenda digitale europea, COM(2010) 245 final, del 19 maggio 2010.
–, Creare uno spazio di libertà, sicurezza e giustizia per i cittadini europei. Piano d'azione per l'attuazione del programma di Stoccolma, COM(2010)171 final, del 20 aprile 2010.
–, Europa 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 final, del 3 marzo 2010.
–, Verso una programmazione congiunta della ricerca: cooperare per affrontare più efficacemente le sfide comuni, COM(2008) 468, del 15 luglio 2008.
–, Un mercato unico per l'Europa del 21esimo secolo, COM(2007) 724 final, del 20 novembre 2007.
–, Verso uno spazio europeo della ricerca, COM(2000) 6 final, del 18 gennaio 2000.
Comunicazione della Commissione al Parlamento europeo e al Consiglio, Seconda relazione sull'applicazione del regolamento generale sulla protezione dei dati, COM(2024) 357 final, del 25 luglio 2024.
–, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, COM(2020) 264 final, del 24 giugno 2020.
Comunicazione della Commissione al Consiglio europeo, Un'agenda dei cittadini – Per un'Europa dei risultati, COM(2006) 211 final, del 10 maggio 2006.
Comunicazione della Commissione al Consiglio, La revisione dell'Europa per il XXI secolo, COM(2007) 412 final, del 10 luglio 2007.
Comunicazione della Commissione europea, Europa 2020: Una strategia per una crescita intelligente, sostenibile e inclusiva, COM(2010) 2020 final, del 3 marzo 2010.
– Costruire un'economia dei dati europea, COM(2017) 09 final, del 10 gennaio 2017.
Conclusioni del Consiglio su un nuovo spazio europeo della ricerca, del 1° dicembre 2020.
– su una medicina personalizzata per i pazienti, del 17 dicembre 2015.
– sulla crisi economica e sull'assistenza sanitaria, del 10 luglio 2014.
– sul processo di riflessione su sistemi sanitari moderni, adeguati e sostenibili, del 10 dicembre 2013.
– sull'avvio del "Processo Lubiana", Verso la piena realizzazione del SER, del 30 maggio 2008 e conclusioni del Consiglio sulla definizione di una visione per lo spazio europeo della ricerca 2020, del 2 dicembre 2008.

– sui valori e sui principi comuni dei sistemi sanitari dell'Unione europea (2006/C 146/01).
Dichiarazione europea sui diritti e i principi digitali per il decennio digitale, COM(2022) 28 final, del 26 gennaio 2022.
Documento di lavoro dei servizi della Commissione sugli spazi comuni europei di dati, SWD(2024) 21 final, del 24 gennaio 2024.
– sulla valutazione d'impatto che accompagna il documento regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari, SWD(2022) 131 final, del 3 maggio 2022.
– che accompagna la Comunicazione della Commissione al Parlamento europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, SWD(2020) 115 final, del 24 giugno 2020.
– che accompagna la Comunicazione della Commissione europea, Un nuovo SER per la ricerca e l'innovazione, SWD(2020) 214 final, del 30 luglio 2020.
– sulla valutazione d'impatto che accompagna il documento proposta di regolamento generale sulla protezione dei dati e proposta di direttiva concernente la tutela 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 di esecuzione di sanzioni penali, e la libera circolazione di tali dati, SEC(2012) 73 final, del 25 gennaio 2012.
Libro verde della Commissione sulla sanità mobile ("mHealth"), COM(2014) 219 final, del 10 aprile 2014.
– sulle nuove prospettive per lo spazio europeo della ricerca, COM(2007) 161 final, del 4 aprile 2007.
Posizione del Consiglio in merito all'applicazione del regolamento generale sulla protezione dei dati (regolamento generale sulla protezione dei dati) (14994/2/19 REV 2), del 15 gennaio 2020.
Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela 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, e la libera circolazione di tali dati, COM(2012) 10 final, del 25 gennaio 2012.
– relativa ai servizi nel mercato interno [SEC(2003) 21], COM(2004) 0002 final, del 25 febbraio 2004.
Proposta di regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2017/745 e (UE) 2017/746 per quanto riguarda la semplificazione e la riduzione degli oneri derivanti dalle norme relative ai dispositivi medici e ai dispositivi medico-diagnostici in vitro, e che modifica il regolamento (UE) 2022/123 per quanto riguarda il sostegno dell'Agenzia europea per i medicinali ai gruppi di esperti sui dispositivi medici e il regolamento (UE) 2024/1689 per quanto riguarda l'elenco della legislazione di armonizzazione dell'Unione di cui al suo allegato I, COM(2025) 1023 final, del 16 dicembre 2025.
– che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 e delle 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 della direttiva (UE) 2019/1024 (*Digital Omnibus*), COM(2025) 837 final, del 19 novembre 2025.
– che modifica i regolamenti (UE) 2016/679, (UE) 2016/1036, (UE) 2016/1037, (UE) 2017/1129, (UE) 2023/1542 e (UE) 2024/573 per quanto riguarda l'estensione di alcune misure attenuanti disponibili per le piccole e medie imprese, alle piccole imprese a media capitalizzazione e ulteriori misure di semplificazione, COM(2025)501 final, del 21 maggio 2025.
– che stabilisce norme procedurali aggiuntive relative all'applicazione del regolamento (UE) 2016/679, COM/2023/348 final, del 4 luglio 2023.
– sullo spazio europeo dei dati sanitari, COM(2022) 197 final, del 3 maggio 2022.
– sui parametri di qualità e sicurezza per le sostanze di origine umana destinate all'applicazione sugli esseri umani e che abroga le direttive 2002/98/CE e 2004/23/CE, COM(2022) 338 final, del 14 luglio 2022.
– riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), COM(2022) 68 final, del 23 febbraio 2022.
– che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM(2021) 206 final, del 21 aprile 2021.
– relativo alla governance europea dei dati (Atto sulla governance dei dati), COM(2020) 767 final, del 25 novembre 2020.
– relativo all'istituzione di un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 e che abroga il regolamento (UE) n. 282/2014 (EU4Health), COM(2020) 405 final, del 28 maggio 2020.
– relativo alla valutazione delle tecnologie sanitarie, che modifica la direttiva 2011/24/UE, COM(2018) 51 final, del 31 gennaio 2018.

Proposta modificata di direttiva del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, COM(92) 422 final, del 15 ottobre 1992.

Raccomandazione (UE) 2020/1475 del Consiglio del 13 ottobre 2020 per un approccio coordinato alla limitazione della libertà di circolazione in risposta alla pandemia di COVID-19, *GU L 337 del 14.10.2020, pp. 3-9.*

Raccomandazione (UE) 2019/243 della Commissione, del 6 febbraio 2019, relativa a un formato europeo di scambio delle cartelle cliniche elettroniche, C(2019) 800, *GU L 39 dell'11.2.2019, pp. 18-27.*

Relazione della Commissione sull'applicazione dei principi di sussidiarietà e proporzionalità e sulle relazioni con i parlamenti nazionali, COM(2023) 640 final, del 12 ottobre 2023.

–, Tutela dei diritti fondamentali nell'era digitale – Relazione annuale 2021 sull'applicazione della Carta dei diritti fondamentali dell'Unione europea, COM(2021) 819 final, del 10 dicembre 2021.
– sull'attuazione della direttiva sulla protezione dei dati (95/46/CE), COM(2003) 265 final, del 15 maggio 2003.

Relazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento della direttiva 2011/24/UE concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera, COM(2022) 210 final, del 12 maggio 2022.

– sullo spazio europeo della ricerca: Progredire insieme nell'Europa della ricerca e dell'innovazione, COM(2019) 83.

– sullo spazio europeo della ricerca: Tempo di attuazione e monitoraggio dei progressi. Relazione sullo stato di avanzamento del SER 2016, COM(2017) 35, del 26 gennaio 2017.
– sui progressi sullo spazio europeo della ricerca, COM(2014) 575 final, del 15 settembre 2014.

Report di sintesi della consultazione pubblica del 27 gennaio 2022, Ares(2022)636543.

Risoluzione del Parlamento europeo del 22 novembre 2023 sui progetti del Parlamento europeo intesi a modificare i Trattati (2022/2051(INL)).
– del 9 giugno 2022 sulla richiesta di convocare una Convenzione per la revisione dei Trattati (2022/2705(RSP)).
– del 3 maggio 2022 sull'intelligenza artificiale in un'era digitale (2020/2266(INI)).
– del 16 febbraio 2022 su rafforzare l'Europa nella lotta contro il cancro – Verso una strategia globale e coordinata (2020/2267(INI)).
– dell'8 luglio 2021 su un nuovo spazio europeo della ricerca e dell'innovazione (2021/2524(RSP)).
– del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP)).
– del 10 luglio 2020 sulla strategia dell'UE in materia di sanità pubblica dopo la crisi della COVID-19 (2020/2691(RSP)).
– del 4 luglio 2013 sul completamento del mercato unico digitale (2013/2655(RSP)).
– del 20 aprile 2012 sull'eGovernment come elemento trainante di un mercato unico digitale europeo (2011/2178(INI)).
– del 6 aprile 2011 sulla governance e il partenariato nel mercato unico (2010/2289(INI)), sul mercato unico per gli europei (2010/2278(INI)) e sul mercato unico per le imprese e la crescita (2010/2277(INI)).
– del 20 maggio 2010 sulla creazione di un mercato unico per i consumatori e i cittadini (2010/2011(INI)).

Valutazione d'impatto iniziale della Commissione sul DA, Ref. Ares(2021)3527151, del 28 maggio 2021.

Legislazione nazionale

Code de la santé publique, del 14 maggio 2021.

Décret n° 2019-536, del 29 maggio 2019.

Decreto del Ministero della Salute del 31 dicembre 2024, Istituzione dell'Ecosistema dei dati sanitari.

Decreto del Ministero della Salute del 7 settembre 2023, Fascicolo sanitario elettronico 2.0.

Decreto del Presidente del Consiglio dei ministri del 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico.

Decreto legge del 2 marzo 2024, n. 19, convertito con modificazioni dalla l. del 29 aprile 2024, Ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza.

Decreto legge del 27 gennaio 2022, n. 4, Misure urgenti in materia di sostegno alle imprese e agli operatori economici, di lavoro, salute e servizi territoriali, connesse all'emergenza da COVID-19, nonché per il contenimento degli effetti degli aumenti dei prezzi nel settore elettrico.

Decreto legge dell'8 ottobre 2021, n. 139, Disposizioni urgenti per l'accesso alle attività culturali, sportive e ricreative, nonché per l'organizzazione di pubbliche amministrazioni e in materia di protezione dei dati personali, convertito con modificazioni dalla legge n. 205/2021.
Decreto legge del 19 maggio 2020, n. 34, convertito con modificazioni in legge del 17 luglio 2020, n. 77, Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da Covid-19.
Decreto legge del 17 marzo 2020, n. 18, Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da Covid-19.
Decreto legge del 9 marzo 2020, n. 14, Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza Covid-19.
Decreto legge del 18 ottobre 2012, n. 179, Ulteriori misure urgenti per la crescita del Paese, convertito con modificazione dalla legge del 17 dicembre 2012, n. 221.
Decreto legislativo del 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
Decreto ministeriale del 20 maggio 2022, Adozione delle Linee guida per l'attuazione del FSE.
Legge del 23 settembre 2025, n. 132, Disposizioni e deleghe del Governo in materia di intelligenza artificiale.
Legge del 22 marzo 2019, n. 29, Istituzione e disciplina della Rete nazionale dei registri e dei tumori e dei sistemi di sorveglianza e del referto epidemiologico per il controllo sanitario della popolazione.
Legge del 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
Loi 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
Loi 78-17/78 relative à l'informatique, aux fichiers et aux libertés.
Finnish Secondary Use of Health and Social Data, 26 aprile 2019.
Gesundheitsdatennutzungsgesetz, 25 marzo 2024.

GIURISPRUDENZA

Corte di giustizia

Parere 1/15 della Corte, emesso ai sensi dell'art. 218, par. 11, TFUE, del 26 luglio 2017, ECLI:EU:C:2016:656.
Parere 2/13 della Corte, emesso ai sensi dell'art. 218, par. 11, TFUE, del 18 dicembre 2014, ECLI:EU:C:2014:2454.
Parere 2/94 della Corte del 28 marzo 1996 sull'adesione della Comunità alla Convenzione dei diritti dell'uomo e delle libertà fondamentali, ECLI:EU:C:1996:140.
Sentenza della Corte del 19 marzo 2026, causa C-526/24, *Brillen Rottler*, ECLI:EU:C:2026:216
– del 2 dicembre 2025, causa C-492/23, *Russmedia Digital*, ECLI:EU:C:2025:935.
– del 4 settembre 2025, causa C-655/23, *Quirin Privatbank*, ECLI:EU:C:2025:655.
– del 4 settembre 2025, causa C-413/23, *EDPS c. CRU*, ECLI:EU:C:2025:645.

– del 29 aprile 2025, causa C-181/23, *Commissione c. Malta*, ECLI:EU:C:2025:283.
– del 3 aprile 2025, causa C-710/23, *Ministerstvo zdravotnictví (Dati riguardanti il rappresentante di una persona giuridica)*, EU:C:2025:231.
– del 27 febbraio 2025, causa C-203/22, *CK*, ECLI:EU:C:2025:117.
– 29 gennaio 2025, cause riunite T-70/23, T-84/23 e T-111/23, *Data Protection Commission c. EDPB*, ECLI:EU:T:2025:116.
– del 9 gennaio 2025, causa C-394/23, *Mousse*, EU:C:2025:2.
– del 4 ottobre 2024, causa C-507/23, *Patērētāju tiesību aizsardzības centrs*, ECLI:EU:C:2024:854.
– del 4 ottobre 2024, causa C-21/23, *Lindenapotheke*, ECLI:EU:C:2024:846.
– del 4 ottobre 2024, causa C-200/23, *Agentsia po vpisvaniyata*, ECLI:EU:C:2024:827.
– del 4 ottobre 2024, causa C-446/21, *Schrems (Comunicazione di dati al grande pubblico)*, EU:C:2024:834.
– del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, ECLI:EU:C:2024:857.
– dell'11 luglio 2024, causa C-757/22, *Meta Platforms Ireland (Action représentative)*, ECLI:EU:C:2024:598.
– del 20 giugno 2024, causa C-590/22, *PS (Indirizzo errato*), EU:C:2024:536.
– del 20 giugno 2024, causa C-182/22 e C-189/22, *Scalable Capital*, EU:C:2024:531.
– dell'11 aprile 2024, causa C-741/21, *juris*, EU:C:2024:288.
– del 7 marzo 2024, causa C-740/22, *Endemol Shine Finland Oy*, ECLI:EU:C:2024:216.
– del 7 marzo 2024, causa C-604/22, *IAB Europe*, ECLI:EU:C:2024:214.
– del 7 marzo 2024, causa C-479/22 P, *OC c. Commissione*, ECLI:EU:C:2024:215.
– del 25 gennaio 2024, causa C-687/21, *MediaMarktSaturn*, ECLI:EU:C:2024:72.
– del 16 gennaio 2024, causa C-33/22, *Österreichische Datenschutzbehörde c. WK*, ECLI:EU:C:2024:46.
– del 21 dicembre 2023, causa C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:1022.
– del 14 dicembre 2023, causa C-456/22, *Gemeinde Ummendorf*, EU:C:2023:988.
– del 14 dicembre 2023, causa C-340/21, *Natsionalna agentsia za prihodite*, ECLI:EU:C:2023:986.
– del 7 dicembre 2023, causa C-634/21, *Schufa Holding*, ECLI:EU:C:2023:957.
– del 5 dicembre 2023, causa C-128/22, *Nordic Info BV*, ECLI:EU:C:2023:951.
– del 5 dicembre 2023, causa C-683/21, *Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos*, ECLI:EU:C:2023:949.
– del 9 novembre 2023, causa C-319/22, *Scania*, ECLI:EU:C:2023:837.
– del 26 ottobre 2023, causa C-307/22, *FT (Copie di cartelle cliniche)*, ECLI:EU:C:2023:811.
– del 5 ottobre 2023, causa C-659/22, *Ministerstvo zdravotnictví (Applicazione mobile Covid-19)*, ECLI:EU:C:2023:745.
– del 4 luglio 2023, causa C-252/21, *Meta Platforms e a*., ECLI:EU:C:2023:537.
– del 22 giugno 2023, causa C-579/21, *Pankki S*, ECLI:EU:C:2023:501.
– del 5 giugno 2023, causa C-204/22, *Commissione europea c. Repubblica di Polonia (Indipendenza e privacy dei giudici)*, ECLI:EU:C:2023:442.
– del 4 maggio 2023, causa C-487/21, *Österreichische Datenschutzbehörde e CRIF*, EU:C:2023:369.

– del 4 maggio 2023, causa C-60/22, *Bundesrepublik Deutschland (Casella di posta elettronica degli uffici giudiziari)*, EU:C:2023:373.
– del 4 maggio 2023, causa C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2023:370.
– del 24 aprile 2023, causa C-492/21 P, *Casa Regina Apostolorum*, ECLI:EU:C:2023:354.
– del 9 febbraio 2023, *X-FAB Dresden*, C-453/20, EU:C:2023:79.
– del 12 gennaio 2023, causa C-154/21, *RW c. Österreichische Post AG*, ECLI:EU:C:2023:3.
– dell'8 dicembre 2022, causa C-460/20, *Google (Ricerca di contenuti presumibilmente inesatti)*, ECLI:EU:C:2022:962.
– dell'11 novembre 2022, causa C-61/19, *Orange Romania*, ECLI:EU:C:2020:901.
– del 27 ottobre 2022, causa C-129/21, *Proximus*, ECLI:EU:C:2022:833.
– del 20 ottobre 2022, causa C-306/21, *Koalitsia "Demokratichna Bulgaria – Obedinenie"*, ECLI:EU:C:2022:813.
– del 7 settembre 2022, causa C-391/20, *Cilevičs*, ECLI:EU:C:2022:638.
– del 1° agosto 2022, causa C-184/20, *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601.
– del 21 giugno 2022, causa C-817/19, *Ligue des droits humains ASBL*, ECLI:EU:C:2022:491.
– del 28 aprile 2022, causa C-319/20, *Meta Platforms I*, ECLI:EU:C:2022:322.
– del 24 febbraio 2022, causa C-175/20, *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, ECLI:EU:C:2022:124.
– del 16 febbraio 2022, causa C-157/21, *Repubblica di Polonia e Ungheria c. Parlamento europeo e Consiglio dell'Unione*, ECLI:EU:C:2022:98.
– del 16 febbraio 2022, causa C-156/21, *Ungheria c. Parlamento e Consiglio*, ECLI:EU:C:2022:97.
– del 22 giugno 2021, causa C-439/19, *Latvijas Republikas Saeima (punti di penalità)*, EU:C:2021:504.
– del 17 giugno 2021, causa C-597/19, *M.I.C.M.*, ECLI:EU:C:2021:492.
– del 15 giugno 2021, causa C-645/19, *Facebook Ireland*, ECLI:EU:C:2021:483.
– del 2 marzo 2021, causa C-746/18, *H.K. c. Prokuratuur*, ECLI:EU:C:2021:152.
– dell'8 dicembre 2020, causa C-626/18, *Polonia c. Parlamento e Consiglio*, ECLI:EU:C:2020:1000.
– dell'8 dicembre 2020, causa C-620/18, *Ungheria c. Parlamento e Consiglio*, ECLI:EU:C:2020:1001.
– del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*, ECLI:EU:C:2020:791.
– del 6 ottobre 2020, causa C-623/17, *Privacy International*, ECLI:EU:C:2020:790.
– del 16 luglio 2020, causa C-311/18, *Schrems II*, ECLI:EU:C:2020:559.
– del 9 luglio 2020, causa C-272/19, *Land Hessen*, ECLI:EU:C:2020:535.
– dell'11 dicembre 2019, causa C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, EU:C:2019:1064.
– del 3 dicembre 2019, causa C-482/17, *Repubblica ceca c. Parlamento e Consiglio*, ECLI:EU:C:2019:1035.
– del 5 novembre 2019, causa C-192/18, *Commissione c. Polonia*, ECLI:EU:C:2019:924.
– del 1° ottobre 2019, causa C-673/17, *Planet 49*, ECLI:EU:C:2019:801.
– del 24 settembre 2019, causa C-507/17*, Google LLC c. CNIL*, ECLI:EU:C:2019:772.

– del 24 settembre 2019, causa C-136/17, *GC e a. c. CNIL*, ECLI:EU:C:2019:773.
– del 29 luglio 2019, causa C-40/17, *Fashion ID*, ECLI:EU:C:2019:629.
– del 14 febbraio 2019, causa C-345/17, *Buivids*, EU:C:2019:122.
– del 25 luglio 2018, causa C-220/18 PPU, *ML c. Generalstaatsanwaltschaft Bremen*, ECLI:EU:C:2018:589.
– del 10 luglio 2018, causa C-25/17, *Jehovan todistajat*, EU:C:2018:551.
– del 20 dicembre 2017, causa C-434/16, *Nowak*, EU:C:2017:994.
– del 27 settembre 2017, causa C-73/16, *Puškár*, EU:C:2017:725.
– del 4 maggio 2017, causa C-13/16, *Rīgas satiksme*, EU:C:2017:336.
– del 9 marzo 2017, causa C-398/15, *Manni*, EU:C:2017:197.
– del 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige*, ECLI:EU:C:2016:970.
– del 19 ottobre 2016, causa C-582/14, *Breyer*, EU:C:2016:779.
– del 21 dicembre 2016, causa C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:970.
–, del 28 luglio 2016, causa C-191/15, *Verein für Konsumenteninformation c. Amazon EU*, ECLI:EU:C:2016:612.
– del 4 maggio 2016, causa C-547/14, *Philip Morris*, ECLI:EU:C:2016:325.
– del 4 maggio 2016, causa C-477/14, *Pillbox*, ECLI:EU:C:2016:324.
– del 4 maggio 2016, causa C-358/14, *Repubblica di Polonia c. Parlamento e Consiglio*.
– del 5 aprile 2016, cause riunite C-404/15 e C-659/15 PPU, *Pál Aranyosi e Robert Căldăraru*, ECLI:EU:C:2016:198
– del 6 ottobre 2015, causa C-362/14, *Schrems I*, ECLI:EU:C:2015:650.
– del 1° ottobre 2015, causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639.
– del 3 settembre 2015, causa C-398/13 P, *Inuit Tapiriit Kanatami e a./Commissione*, EU:C:2015:535.
– del 16 giugno 2015, causa C-62/14, *Gauweiler e a.*, EU:C:2015:400.
– del 29 aprile 2015, causa C-528/13, *Léger*, ECLI:EU:C:2015:288.
– del 28 gennaio 2015, causa C-375/13, *Kolassa*, ECLI:EU:C:2015:37.
– dell'11 dicembre 2014, causa C-212/13, *Ryneš*, EU:C:2014:2428.
– del 17 luglio 2014, causa C-141/12 e C-372/12, *YS e Minister voor Immigratie, Integratie en Asiel*, EU:C:2014:2081.
– del 13 maggio 2014, causa C-131/12, *Google Spain*, ECLI:EU:C:2014:317.
– dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238.
– del 30 maggio 2013, causa C-342/12, *Worten*, EU:C:2013:355.
– del 22 gennaio 2013, causa C-283/2011, *Sky Östrerreich GmbH c. Österreichischer Rundfunk*, ECLI:EU:C:2013:28.
– del 6 settembre 2012, causa C-544/10, *Deuthches Weintor*, ECLI:EU:C:2012:526.
– del 19 luglio 2012, causa C-130/10, *Parlamento c. Consiglio*, ECLI:EU:C:2012:472.
– del 19 aprile 2012, causa C-461/10, *Bonnier*, ECLI:EU:C:2012:219.
– del 24 novembre 2011, cause riunite C-468/10 e C-469/10, *ASNEF*, ECLI:EU:C:2011:777.
– del 27 ottobre 2011, causa C-255/09, *Commissione c. Portogallo*, ECLI:EU:C:2011:695.
– del 17 marzo 2011, causa C-221/09, *AJD Tuna*, EU:C:2011:153.
– del 9 marzo 2010, causa C-518/07, *Commissione c. Germania*, ECLI:EU:C:2010:12.

– dell'8 marzo 2011, causa C-34/09, *Zambrano*, ECLI:EU:C:2011:124.
– del 27 gennaio 2011, causa C-490/09, *Commissione c. Lussemburgo*, ECLI:EU:C:2011:34.
– del 22 dicembre 2010, causa C-208/09, *Sayn-Wittgenstein*, ECLI:EU:C:2010:806.
– del 9 novembre 2010, cause riunite C-92/09 e C-93/09, *Volker*, ECLI:EU:C:2010:662.
– del 5 ottobre 2010, causa C-173/09, *Elchinov*, ECLI:EU:C:2010:581.
– del 5 ottobre 2010, causa C-512/08, *Commissione c. Francia*, ECLI:EU:C:2010:579.
– dell'8 giugno 2010, causa C-58/08, *Vodafone*, ECLI: ECLI:EU:C:2010:321.
– del 1° giugno 2010, cause riunite C-570 e C-571/07, *Blanco Pérez*, ECLI:EU:C:2010:300.
– del 19 gennaio 2010, causa C-555/07, *Kücükdeveci*, ECLI:EU:C:2010:21.
– del 1° ottobre 2009, causa C-370/07, *Commissione c. Consiglio*, ECLI:EU:C:2009:590.
– del 7 maggio 2009, causa C-553/07, *Rijkeboer*, ECLI:EU:C:2009:25.
– del 16 dicembre 2008, causa C-73/07, *Satakunnan Markkinapörssi e Satamedia*, ECLI:EU:C:2008:727.
– dell'11 settembre 2008, causa C-141/07, *Commissione c. Germania*, ECLI:EU:C:2008:492.
– del 3 settembre 2008, cause riunite C-402/05 P e C-415/05 P, *Kadi*, ECLI:EU:C:2008:461.
– del 29 gennaio 2008, causa C-275/06, *Promusicae*, ECLI:EU:C:2008:54.
– del 19 aprile 2007, causa C-444/05, *Stamatelaki*, ECLI:EU:C:2007:231.
– del 12 dicembre 2006, causa C-380/03, *Repubblica di Germania c. Parlamento e Consiglio*, ECLI:EU:C:2006:772.
– del 16 maggio 2006, causa C-372/04, *Watts*, ECLI:EU:C:2006:325.
– del 10 gennaio 2006, causa C-178/03, *Commissione c. Parlamento e Consiglio*, ECLI:EU:C:2006:4.
– del 20 gennaio 2005, causa C-27/02, *Engler*, ECLI:EU:C:2005:33.
– del 14 dicembre 2004, causa C-210/03, *Swedish Match*, ECLI:EU:C:2004:802.
– del 14 dicembre 2004, causa C-434/02, *Arnold André*, ECLI:EU:C:2004:800.
– del 14 ottobre 2004, causa C-36/02, *Omega*, ECLI:EU:C:2004:614.
– del 9 settembre 2004, cause riunite C-184/02 e C-223/02, *Spagna e Finlandia/Parlamento e Consiglio*, ECLI:EU:C:2004:497.
– del 29 aprile 2004, causa C-338/01, *Commissione c. Consiglio*, ECLI:EU:C:2004:253.
– del 18 marzo 2004, causa C-8/02, *Leichtle*, ECLI:EU:C:2004:161.
– del 6 novembre 2003, causa C-101/01, *Lindqvist*, ECLI:EU:C:2003:596.
– del 23 ottobre 2003, causa C-56/01, *Inizan*, ECLI:EU:C:2003:578.
– del 12 giugno 2003, causa C-112/00, *Schmidberger*, ECLI:EU:C:2003:333.
– del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01, *Rundfunk*, ECLI:EU:C:2003:294.
– del 13 maggio 2003, causa C-385/99, *Müller-Fauré e van Riet*, ECLI:EU:C:2003:270.
– del 17 settembre 2002, causa C-334/00, *Tacconi*, ECLI:EU:C:2002:499.
– del 12 dicembre 2002, causa C-281/01, *Commissione c. Consiglio*, ECLI:EU:C:2002:761.
– del 10 dicembre 2002, causa C-491/01, *British American Tobacco*, ECLI:EU:C:2002:741.
– del 25 luglio 2002, causa C-50/00 P, *Unión de Pequeños Agricultores*, ECLI:EU:C:2002:462.

– del 12 luglio 2001, causa C-157/99, *Smits e Peerbooms*, ECLI:EU:C:2001:404.
– del 9 ottobre 2001, causa C-377/98, *Paesi Bassi/Parlamento e Consiglio*, ECLI:EU:C:2001:523.
– del 30 gennaio 2001, causa C-36/98, *Spagna c. Consiglio*, ECLI:EU:C:2001:64.
– del 5 ottobre 2000, causa C-376/98, *Germania c. Parlamento europeo e Consiglio (Tobacco Advertising)*, EU:C:2000:544.
– del 25 febbraio 1999, cause riunite C-164 e 165/97, *Parlamento c. Consiglio*, ECLI:EU:C:1999:99.
– del 27 ottobre 1998, causa C-51/97, *Réunion européenne*, ECLI:EU:C:1998:509.
– del 19 novembre 1998, causa C-150/94, *Regno Unito/Consiglio,* EU:C:1998:547.
– del 28 aprile 1998, causa C-158/96, *Kohll*, ECLI:EU:C:1998:171.
– del 28 aprile 1998, causa C-120/95, *Decker*, ECLI:EU:C:1998:167.
– del 9 dicembre 1997, causa C-265/95, *Commissione c. Francia*, ECLI:EU:C:1997:595.
– del 17 giugno 1997, causa 70/95, *Sodemare e a*., ECLI:EU:C:1997:301.
– del 13 maggio 1997, causa C-233/94, *Germania/Parlamento e Consiglio*, ECLI:EU:C:1997:231.
– del 12 novembre 1996, causa C-84/94, *Regno Unito e Irlanda del Nord c. Consiglio*, ECLI:EU:C:1996:431.
– del 26 marzo 1996, causa C-271/94, *Parlamento c. Consiglio*, ECLI:EU:C:1996:133.
– del 9 ottobre 1995, causa C-426/93, *Repubblica federale della Germania c. Consiglio*, ECLI:EU:C:1995:367.
– del 28 giugno 1994, causa C-187/93, *Parlamento c. Consiglio*, ECLI:EU:C:1994:265.
– del 17 marzo 1993, causa C-155/91, *Commissione c. Consiglio*, ECLI:EU:C:1993:98.
– del 17 giugno 1992, causa C-26/91, *Handte*, ECLI:EU:C:1992:268.
– del 18 giugno 1991, causa C-260/89, *ERT*, ECLI:EU:C:1991:254.
– dell'11 giugno 1991, causa C-300/89, *Commissione c. Consiglio*, ECLI:EU:C:1991:244.
– del 13 luglio 1989, causa C-5/88, *Wachauf*, ECLI:EU:C:1989:321.
– del 21 giugno 1988, causa 197/1988, *Brown*, ECLI:EU:C:1988:323.
– del 23 febbraio 1988, causa C-68/86, *Regno Unito e Irlanda del Nord c. Consiglio*, ECLI:EU:C:1988:85.
– del 23 aprile 1986, causa 294/83, *Les Verts*, ECLI:EU:C:1986:166.
– del 7 febbraio 1984, causa 238/82, *Duphar e a*., ECLI:EU:C:1984:45.
– del 20 febbraio 1979, causa C-120/78, *Rewe-Zentral*, ECLI:EU:C:1979:42.
– dell'11 luglio 1974, causa C-8/74, *Dassonville*, ECLI:EU:C:1974:82.
– del 17 dicembre 1970, causa C-11/70, *Internationale Handelsgesellschaft*, ECLI:EU:C:1970:114.
– del 10 dicembre 1969, cause riunite C-6/69 e C-11/69, *Commissione c. Francia*, ECLI:EU:C:1969:68.
– del 12 novembre 1969, causa C-29/69, *Stauder*, ECLI:EU:C:1969:57.
– del 5 febbraio 1963, causa C-26/62, *van Gend en Loos*, ECLI:EU:C:1963:1.

Tribunale

Sentenza del Tribunale del 26 aprile 2023, causa T-557/20, *CRU c. EDPS*, ECLI:EU:T:2023:219.
– del 13 luglio 2022, causa T-227/21, *Illumina c. Commissione*, ECLI:EU:T:2022:447.
– del 3 dicembre 2015, causa T-343/13, *CN c. EDPS*, ECLI:EU:T:2015:926.

Conclusioni degli Avvocati generali

Conclusioni dell'Avvocato generale Szpunar del 25 aprile 2024, causa C-21/23, *Lindenapotheke*, ECLI:EU:C:2024:354.

– Campos Sánchez Bordona del 25 maggio 2023, causa C-667/21, *Krankenversicherung Nordrhein*, ECLI:EU:C:2023:433.
– Szpunar dell'11 maggio 2023, causa C-33/22, *Österreichische Datenschutzbehörde c. WK*, ECLI:EU:C:2023:397.
– Emiliou del 20 aprile 2023, causa C-307/22, *FT (Copie di cartelle cliniche)*, ECLI:EU:C:2023:315.
– Ćapeta del 30 marzo 2023, causa C-106/22, *Xella*, ECLI:EU:C:2023:267.
– Pikamäe del 16 marzo 2023, causa C-634/21, *Schufa Holding (Scoring)*, ECLI:EU:C:2023:220.
– Campos Sánchez-Bordona del 6 ottobre 2022, causa C-300/21, *UI c. Österreichische Post AG*, ECLI:EU:C:2022:756.
– Pikamäe del 31 marzo 2022, causa C-77/21, *Digi*, ECLI:EU:C:2022:248.
– Pitruzzella del 27 gennaio 2022, causa C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:65.
– de La Tour del 2 dicembre 2021, causa C-319/20, *Meta Platforms Ireland*, ECLI:EU:C:2021:979.
– Bobek del 6 ottobre 2021, causa C-245/20, *Autoriteit Persoonsgegevens*, ECLI:EU:C:2021:822.
– Bobek del 2 settembre 2021, causa C-175/20, *Valsts ieņēmumu dienests (Trattamento di dati personali a fini fiscali)*, ECLI:EU:C:2021:690.
– Jääskinen del 25 giugno 2013, causa 131/12, *Google Spain*, ECLI:EU:C:2013:424.
– Bot del 10 marzo 2011, causa C-34/10, *Brüstle c. Greenpeace*, ECLI:EU:C:2011:138.
– Sharpston del 17 giugno 2010, cause riunite C-92/09 e C-93/09, *Volker*, ECLI:EU:C:2010:353.
– Ruiz-Jarabo Colomer del 22 dicembre 2008, causa C-212/13, *Ryneš*, ECLI:EU:C:2008:773.
– Ruiz-Jarabo Colomer dell'11 gennaio 2007, causa C-444/05, *Stamatelaki*, ECLI:EU:C:2007:24.
– Tizzano del 19 settembre 2002, causa C-101/01, *Lindqvist*, ECLI:EU:C:2002:513.
– Tizzano del 14 novembre 2002, cause riunite C-465/00, C-138/01 e C-139/01, *Rundfunk*, ECLI:EU:C:2002:662.
– Tesauro del 16 settembre 1997, cause C-120/95 e C-158/96, *Decker e Kohll*, ECLI:EU:C:1997:399.

MONOGRAFIE

ADAM R., TIZZANO A., *Lineamenti di diritto dell'Unione europea*, Giappichelli, Torino, 2022.

–, *Manuale di diritto dell'Unione europea*, Giappichelli, Torino, 2020.

AMALFITANO C., *General Principles of EU Law and the Protection of Fundamental Rights*, Elgar, Cambridge, 2018.

AMALFITANO C., CONDINANZI M., *Paura dell'Europa: spunti di razionalizzazione. Chi ha (ancora) paura dell'Europa?*, Giappichelli, Torino, 2020.

ARENA A., *Il principio della preemption in diritto dell'Unione europea. Esercizio delle competenze e ricognizione delle divergenze tra diritto derivato e diritto nazionale*, Editoriale scientifica, Napoli, 2013.

AURUCCI P., *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Edizioni Scientifiche Italiane, Napoli, 2023.
BARBIERI S., *Il rinvio pregiudiziale tra giudici ordinari e Corte costituzionale. La ragione del conflitto*, Jovene, Napoli, 2024.
BARNARD C., *The Substantive Law of the EU. The Four Freedoms*, OUP, Oxford, 2019.
BENNETT C.J., *Regulating Privacy – Data Protection and Public Policy in Europe and the United States*, Cornell University Press, New York, 1992.
BUSATTA L., *La salute sostenibile. La complessa determinazione del diritto di accedere alle prestazioni sanitarie*, Giappichelli, Torino, 2018.
BRADFORD A., *The Brussels Effect: How the European Union Rules the World*, OUP, Oxford, 2020.
BRAVO F., *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018.
BYGRAVE L.A., *Data Privacy Law: An International Perspective*, OUP, Oxford, 2014.
–, *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, The Hague, 2002.
BURCI G.L., TOEBES B., *Research Handbook on Global Health Law*, Edward Elgar, Cheltenham, 2018.
CAGGIANO G., CONTALDI G., MANZINI P. (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Cacucci, Bari, 2021.
CALIFANO L. et al., *La protezione dei dati personali, natura, garanzie e bilanciamento di un diritto fondamentale*, Giappichelli, Torino, 2023.
CANCILLA F.A., *Servizi del welfare e diritti sociali nella prospettiva dell'integrazione europea*, Giuffrè, Milano, 2009.
CANNIZZARO E., *Il diritto dell'integrazione europea. L'ordinamento dell'Unione*, Giappichelli, Torino, 2022.
CASOLARI F., *Leale cooperazione tra Stati membri e Unione Europea. Studio sulla partecipazione all'Unione al tempo delle crisi*, Editoriale Scientifica, Bologna, 2020.
CATHAOIR K.Ó., *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.
CELESTE E., *Digital Constitutionalism: The Role of Internet Bills of Rights*, Routledge, London, 2023.
CHALMERS D., DAVIES G., MONTI G., *European Union Law. Cases and Materials*, CUP, Cambridge, 2010.
CHITI M.P., NATALINI A. (a cura di), *Lo Spazio amministrativo europeo. Le pubbliche amministrazioni dopo il Trattato di Lisbona*, Il Mulino, Bologna, 2012.
CICIRIELLO M.C., *L'Unione europea e i suoi principi giuridici*, Editoriale scientifica, Napoli, 2010.
COLLMANN J., MATEI S.A., *Ethical Reasoning in Big Data: An Exploratory Analysis*, Springer, New York, 2016.
CORTEN O., *Méthodologie du droit international public*, Éditions de l'Université de Bruxelles, Bruxelles, 2009.
COSTAMAGNA F., *I servizi socio-sanitari nel mercato interno europeo. L'applicazione delle norme dell'Unione europea in materia di concorrenza, aiuti di Stato e libera circolazione dei servizi*, Edizioni Scientifiche Italiane, Napoli, 2011.
CRAIG P., DE BÚRCA G., *EU Law: Text, Cases, and Materials*, OUP, Oxford, 2020.

DAWSON M., DE WITTE F., *EU Law and Governance*, CUP, Cambridge, 2022.
DE GREGORIO G., *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, CUP, Cambridge, 2022.
DE GROVE VALDEYRON N. (sous la direction de), *Espace européen des données de santé et IA: enjeux juridiques et défis de mise en œuvre*, Presses de l'Université Toulouse Capitole, 2025.
DE PASQUALE P., *Il principio di sussidiarietà nell'ordinamento comunitario*, Editoriale scientifica, Napoli, 2000.
DERMINE P., *Le plan de relance "Next Generation EU" de l'Union européenne – Analyse constitutionnelle d'une initiative historique*, Bruylant, Bruxelles, 2023.
DE RUIJTER A., *EU Health Law & Policy: The Expansion of EU Power in Public Health and Health Care*, OUP, Oxford, 2019.
DE SOUSA P.C., *The European Fundamental Freedoms: A Contextual Approach*, OUP, Oxford, 2015.
DI FEDERICO G., *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*, Springer, Dordrecht, 2011.
DI FEDERICO G., NEGRI S., *Unione europea e salute. Principi, azioni, diritti e sicurezza*, Cedam, Milano, 2019.
DOUGLAS-SCOTT S., *Constitutional Law of the European Union*, Pearson Education Limited, London, 2002.
FERRARO F., IANNONE C., *Il rinvio pregiudiziale*, Giappichelli, Torino, 2020.
FERRI F., *Il bilanciamento tra diritti fondamentali nel mercato unico digitale*, Giappichelli, Torino, 2022.
FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Zanichelli, Bologna, 2012.
FLEAR M.L., *Governing Public Health. EU Law, Health and Biopolitics*, Hart Publishing, Oxford, 2015.
GONZÁLEZ FUSTER G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Cham, 2014.
GOSTIN L.O., *Global Health Law*, Harvard University Press, Cambridge, 2014.
GRAGLIA P.S., *Altiero Spinelli*, Il Mulino, Bologna, 2010.
GREER S.L., KURZER P., *European Union Public Health Policy: Regional and Global Trends*, Routledge, London and New York, 2013.
GROPPI T., *Comm. all'art. 52*, in R. BIFULCO, M. CARTABIA, A. CELOTTO, *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, il Mulino, Bologna, 2001.
GUARDA P., *Il regime giuridico dei dati della ricerca scientifica*, Editoriale scientifica, Napoli, 2021.
GUTWIRTH S. et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009.
HAAS E.B., *The Uniting of Europe: Political, Social and Economic Forces*, 1950-1957, Stevens & Sons, London, 1958.
HEISENBERG D., *Negotiating Privacy: The European Union, The United States, and Personal Data Protection*, Lynne Rienner Pub, Boulder, 2005.
HERVEY T., MCHALE J., *European Union Health Law: Themes and Implications. Law in Context*, CUP, Cambridge, 2015.

–, *Rights: Health Rights as Human Rights, in European Union Health Law: Themes and Implications*, CUP, Cambridge, 2015.
–, *Health Law and the European Union*, OUP, Oxford, 2004.
HIJMANS H., *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, Springer, Cham, 2016.
HORSLEY T., *The Court of Justice of the European Union as an Institutional Actor. Judicial Lawmaking and its Limits*, CUP, Cambridge, 2022.
HUSTINX P., *The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, in Collected Courses of the European University Institute's Academy of European Law*, OUP, Oxford, 2013.
INGRAVALLO I., *L'effetto utile nell'interpretazione del diritto dell'Unione europea*, Cacucci, Bari, 2017.
KELLERBAUER M., KLAMERT M., TOMKIN J. (eds.), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, OUP, Oxford, 2019.
KLAMERT M., *The Principle of Loyalty in EU Law*, OUP, Oxford, 2014.
KOGUT-CZARKOWSKA M., SHABANI M., *Federated Networks and Secondary Uses of Health Data – Challenges in Ensuring Appropriate Safeguards for Sharing Health Data Under the GDPR and EHDS*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Routledge, London, 2025.
KONSTATINIDES K., *Division of Powers in European Union Law – The Delimitation of Internal Competence between the EU and the Member States*, Kluwer Law International, Alphen aan den Rijn, 2009.
KOSTA E., BOEHM F., *The EU Law Enforcement Directive (LED). A Commentary*, OUP, Oxford, 2024.
KOSTA E., *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, Leiden, 2013.
LEONELLI S., *La ricerca scientifica nell'era dei big data. Cinque modi in cui i Big Data danneggiano la scienza, e come salvarla*, Meltemi, Milano, 2018.
LENAERTS K., VAN NUFFEL P., *European Union Law*, Sweet & Maxwell, London, 2011.
LINSKEY O., *The Foundations of EU Data Protection Law*, OUP, Oxford, 2015.
MAMMARELLA G., *Storia d'Europa dal 1945 a oggi*, GLF editori Laterza, Roma, 2006.
MALETIC I., *The Law and Policy of Harmonization in Europe's Internal Market*, Edward Elgar, Cheltenham, 2013.
MORAVCSIK A., *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*, UCL Press, London, 1999.
MOSCHETTA T.M., *Il ravvicinamento delle normative nazionali per il mercato interno*, Cacucci, Bari, 2018.
OBERMAIER A.J., *The End of Territoriality? The Impact of ECJ Rulings on British, German and French Social Policy*, Ashgate, Aldershot, 2009.
PARIS J-C., *The Constitution for Europe: A Legal Analysis*, CUP, Cambridge, 2006.
PASERI L., *Il governo dei dati. Interesse pubblico, altruismo e partecipazione*, Giappichelli, Torino, 2025.
PATRUNO L., *Il modello istituzionale europeo e l'idea di costituzione*, Giappichelli, Torino, 2006.
POCAR F., BARUFFI M.C., ADINOLFI A., *Commentario breve ai Trattati dell'Unione europea*, Cedam, Assago, 2014.

POLLICINO O., *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism*, Hart, Oxford, 2021.
RODOTÀ S., *Tecnologie e diritti*, Il Mulino, Bologna, 2021.
ROSSI L.S. (a cura di), *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, Giuffrè, Milano, 2002.
RUGANI G., *La regolamentazione dei flussi di dati personali dall'UE verso Paesi terzi. Alla ricerca di un bilanciamento tra espansione del commercio internazionale e* personal data protection, Giappichelli, Torino, 2024.
SALMONI F., *Recovery fund, condizionalità e debito pubblico. La grande illusione*, Cedam, Padova, 2021.
SCHNEIDER G., *Health Data Pools Under European Data Protection and Competition Law. Health as a Digital Business*, Springer, Berlin, 2022.
SCHÜTZE R., *European Constitutional Law*, OUP, Oxford, 2021.
–, *From Dual to Cooperative Federalism: The Changing Structure of European Law*, OUP, Oxford, 2009.
SENDEN L., *Soft Law in European Community Law*, Hart Publishing, Oxford, 2004.
SLOKENBERGA S., CATHAOIR K.Ó., SHABANI M. (eds.), *The European Health Data Space. Examining a New Era in Data Protection*, Routledge, London, 2025.
SOLOVE D.J., *The Digital Person: Technology, and Privacy in the Information Age*, NYU Press, New York, 2004.
SOLOVE D.J., SCHWARTZ P.M., *Information Privacy Law*, Wolters Kluwer, Alphen aan den Rijn, 2020.
SPINELLI A., ROSSI E., *Il Manifesto di Ventotene*, Corriere della Sera, Milano, 2011.
STEFFEN M., *Health Governance in Europe: Issues, Challenges and Theories*, Routledge, London and New York, 2005.
TESAURO G., *Diritto dell'Unione europea*, Cedam, Padova, 2012.
TRIDIMAS T., *General Principles of EU Law*, OUP, Oxford, 2006.
TRUCCO L., *Carta dei diritti fondamentali e costituzionalizzazione dell'Unione Europea. Un'analisi delle strategie argomentative e delle tecniche decisorie a Lussemburgo*, Giappichelli, Torino, 2013.
VON BOGDANDY A., *The Emergence of European Society through Public Law: A Hegelian and Anti-Schmittian Approach*, OUP, Oxford, 2024.
WALKER N. (ed.), *Europe's Area of Freedom, Security and Justice*, OUP, Oxford, 2004.
WEATHERILL S., *Law and Values in the European Union*, OUP, Oxford, 2016.
WESTIN A., *Privacy and Freedom*, The Bodley Head, London, 1970.
ZEITLIN J., VANHERCKE B., *Socializing the European Semester? Economic Governance and Social Policy Coordination in Europe 2020*, Sieps, Stockholm, 2014.

CAPITOLI DI MONOGRAFIE

ACQUISTI A., GROSSKLAGS J., *What Can Behavioral Economics Teach Us About Privacy*, in A. ACQUISTI et al. (eds.), *Digital Privacy. Theory, Technologies, and Practices*, New York, Auerbach Publications, 2008.
AIDINLIS S., *Government-to-Business (G2B) Research Data Sharing and the GDPR: Reconciling the 'Public' with the 'Private'?*, in E. KOSTA, R. LEENES, I. KAMARA, *Research Handbook on Privacy and Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022.

AMALFITANO C., FERRI F., *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO, *La trasformazione digitale in Europa. Diritti e principi*, Giappichelli, Torino, 2023.

ARENA A., *The Twin Doctrines of Primacy and Pre-emption*, in R. SCHÜTZE, T. TRIDIMAS (eds.), *Oxford Principles of European Union Law, Vol. I: The European Union Legal Order*, OUP, Oxford, 2018.

AUSTIN L., *Enough About Me: Why Privacy is About Power, Not Consent (or Harm)*, in A. SARAT (ed.), *A World Without Privacy: What Law Can and Should Do?*, CUP, Cambridge, 2014.

AZOULAI L., *The Complex Weave of Harmonization*, in D. CHALMERS, A. ARNULL (eds.), *The Oxford Handbook of European Union Law*, OUP, Oxford, 2015.

BAQUERO CRUZ J., *The Case Law of the European Court of Justice on the Mobility of Patients: An Assessment*, in J.W. VAN GRONDEN et al. (eds.), *Health Care and EU Law*, Springer, The Hague, 2011.

BARTOLONI M.E., *The Horizontal Social Clause in a Legal Dimension*, in F. IPPOLITO, M.E. BARTOLONI, M. CONDINANZI, *The EU and the Proliferation of Integration Principles under the Lisbon Treaty*, Routledge, London, 2019.

BELLITTI G., *Big data e abuso di posizione dominante*, in A. CATRICALÀ, C.E. CAZZATO, F. FIMMANÒ, *Diritto antitrust*, Giuffrè, Milano, 2021.

BENGOETXEA J., MACCORMICK N., SORIANO L.M., *Integration and Integrity in the Legal Reasoning of the European Court of Justice*, in G. DE BÚRCA, J.H.H. WEILER (eds.), *The European Court of Justice*, OUP, Oxford, 2001.

BENTZEN H.B., *Context as Key: The Protection of Personal Integrity by Means of the Purpose Limitation Principle*, in E. KOSTA, R. LEENES, I. KAMARA, *Research Handbook on Privacy and Data Protection Law*, Edward Elgar Publishing, Cheltenham, 2022.

–, *In the Name of Scientific Advancement: How to Assess What Constitutes 'Scientific Research' in the GDPR to Protect Data Subjects and Democracy*, in G. TERZIS et al. (eds.), *Disinformation and Digital Media as a Challenge for Democracy*, Intersentia, Cambridge, 2020.

BOGNETTI G., *The Concept of Human Dignity in European and US Constitutionalism*, in G. NOLTE (ed.), *European and US Constitutionalism*, CUP, Cambridge, 2005.

BRAVO F., *Il principio di solidarietà*, in F. BRAVO (a cura di), *Dati personali, protezione, libera circolazione e governance. I principi*, Pacini Giuridica, Pisa, 2023.

BROWNSWORD R., *Freedom of Contract, Human Rights and Human Dignity*, in D. FRIEDMAN, D. BARAK-EREZ (eds.), *Human Rights in Private Law*, Hart Publishing, London, 2001.

BUSATTA L., *Moving Patients and Families and the Social Rights to Cross-Border Healthcare*, in M. PASCUAL, A. PÉREZ (eds.), *The Right to Family Life in the European Union*, Routledge, London, 2017.

BUTIN D., CHICOTE M., LE MÈTAYER D., *Strong Accountability: Beyond Vague Promises,* in S. GUTWIRTH, R. LEENES, P. DE HERT (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer, Berlin, 2014.

BYGRAVE L.A., WIESE SCHARTUM D., *Consent, Proportionality and Collective Power*, in S. GUTWIRTH et al. (eds.), *op. cit*., 2009.

CAFARI PANICO R., *Principio di sussidiarietà e clausola di flessibilità*, in G. ADINOLFI, A. LANG (a cura di), *Il Trattato che adotta una Costituzione per l'Europa: quali limitazioni all'esercizio dei poteri sovrani degli Stati?*, Giuffrè, Milano, 2006.

CAGGIANO G., *La "filigrana del mercato" nello status di cittadino europeo*, in E. TRIGGIANI (a cura di), *Le nuove frontiere della cittadinanza europea*, Cacucci, Bari, 2011.

CANNIZZARO E., *L'interaction entre objectifs et compétences matérielles dans le système normatif de l'Union européenne*, in E. NEFRAMI (sous la direction de), *Objectifs et compétences dans l'Union européenne*, Bruylant, Bruxelles, 2013.

CARTABIA M., *L'impatto costituzionale della Carta dei diritti fondamentali dell'Unione europea*, in M. CARTABIA (a cura di), *Liber amicum Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice européenne*, 2018.

CECCHETTI C., *Il controllo dei parlamenti nazionali sul rispetto del principio di sussidiarietà*, in G. DI FEDERICO (a cura di), *Alla (ri)scoperta del Parlamento europeo: 1979-2019*, Giappichelli, Torino, 2021.

CERVERA DE LA CRUZ P., SHABANI M., *Fair Enough? Exploring the Role of Fairness in Secondary Uses of Health Data in the European Health Data Space*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

CHEN J.C., DOVE E.S., BHAKUNI H., *Explicit Consent and Alternative Data Protection Processing Grounds for Health Research*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit.*, 2022.

CLEMENTI F., *Lo spazio di libertà, sicurezza e giustizia*, in F. BASSANINI, G. TIBERI, *La Costituzione europea. Un primo commento*, Il Mulino, Bologna, 2004.

COSTAMAGNA F., *Il coordinamento delle politiche economiche nell'ambito del Semestre europeo*, in O. PORCHIA (a cura di), *Governance economica europea. Strumenti dell'Unione, rapporto con l'ordinamento internazionale e ricadute nell'ordinamento interno*, Editoriale Scientifica, Napoli, 2015.

COSTAMAGNA F., *The Internal Market and the Welfare State: Anything New after Lisbon?*, in M. TRYBUS, L. RUBINI (eds.), *The Treaty of Lisbon and the Future of European Law and Policy*, Edward Elgar, Cheltenham, 2012.

DALLA CORTE L., *A Right to a Rule: On the Substance and Essence of the Fundamental Right to Personal Data Protection*, in D. HALLINAN et al. (eds.), *Data Protection and Privacy: Data Protection and Democracy*, Hart Publishing, Oxford, 2020.

DAVIES G., *Originalism at the European Court of Justice*, in I. GOVAERE, S. GARBEN (eds.), *The Internal Market 2.0*, Hart Publishing, Oxford, 2020.

–, *The Competence to Create an Internal Market: Conceptual Poverty and Unbalanced Interests*, in S. GARBEN, I. GOVAERE (eds.), *The Division of Competences Between the EU and the Member States: Reflections on the Past, the Present and the Future*, Hart Publishing, Oxford, 2017.

DE HERT P., *EU Sanctioning Powers and Data Protection: New Tools for Ensuring the Effectiveness of the GDPR in the Spirit of Cooperative Federalism*, in S. MONTALDO, F. COSTAMAGNA, A. MIGLIO (eds.), *EU Law Enforcement. The Evolution of Sanctioning Powers*, Routledge, New York, 2021.

DE HERT P., GUTWIRTH S., *Data Protection in The Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in S. GUTWIRTH et al. (eds.), *op. cit.*, Springer, Berlin, 2009.

DE PASQUALE P., *Commento all'articolo 5 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, 2014.

DE WITTE B., *Integration through Funding – The Union's Finances as a Policy Instrument*, in R. WEBER (ed.), *The Financial Constitution of European Integration – Follow the Money?*, Hart Publishing, London, 2023.

–, *Integration Clauses – A Comparative Epilogue*, in F. IPPOLITO, M.E. BARTOLONI, M. CONDINANZI, *op. cit*., 2019.
–, *Exclusive Member States Competences: Is there Such a Thing?*, in I. GOVAERE, S. GARBEN (eds.), *op. cit.*, 2017.
–, *A Competence to Protect: The Pursuit of Non-market Aims Through Internal Market Legislation*, in P. SYRPIS, *The Judiciary, the Legislature and the Internal Market*, CUP, Cambridge, 2012.
DE TERWANGNE C., *Privacy and Data Protection in Europe: Council of Europe Convention 108 and the European Union's GDPR*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit.*, 2022.
DI FEDERICO G., *Il ruolo del Parlamento europeo nella costruzione del mercato unico digitale*, in G. DI FEDERICO, *op. cit.*, 2021.
–, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in E. AL MUREDEN, C. BOTTARI (eds.), *La salute del futuro: prospettive e nuove sfide del diritto sanitario*, Bononia University Press, Bologna, 2020.
–, *Art. 35*, in R. MASTROIANNI et al. (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017.
–, *Access to Healthcare in the Post-Lisbon Era and the Genuine Enjoyment of EU Citizens' Rights*, in L.S. ROSSI, F. CASOLARI (eds.), *The EU After Lisbon. Amending or Coping with the Existing Treaties?*, Springer, Cham, 2014.
–, *Fundamental Rights in the EU: Legal Pluralism and Multi-Level Protection After the Lisbon Treaty*, in G. DI FEDERICO (ed.), *The EU Charter of Fundamental Rights: From Declaration to Binding Instrument*, Springer, Dordrecht, 2011.
DREXL J., *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, in A. DE FRANCESCHI, R. SCHULZE (eds.), *Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice*, Beck, München, 2019.
DUBOUT E., *The Protection of Fundamental Rights and the Allocation of Competences in the EU: A Clash of Constitutional Logics*, in L. AZOULAI (ed.), *The Question of Competence in the European Union*, OUP, Oxford, 2014.
ECHEVERRÍA E.S., *The European Health Data Space: A New Paradigm for Secondary Uses of Health Data for Scientific Research?*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.
EL ASRY E., MANSNÉRUS J., LIEDE S., *Striking the Balance: Genomic Data, Consent and Altruism in the European Health Data Space*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.
FALCE V., *Art. 20*, in R. D'ORAZIO et al., *Codice della privacy e data protection*, Giuffrè, Milano, 2021.
FERRARO F., LAZZARINI N., *Art. 52. portata e interpretazione dei diritti e dei principi*, in R. MASTROIANNI et al. (a cura di), *op. cit.*, 2017.
FLEAR M.L., *Regulating New Technologies: EU Internal Market Law, Risk and Socio-Technical Order*, in M. CREMONA (ed.), *New Technologies and EU Law*, OUP, Oxford, 2017.
FIORENTINI A., *Vers la mise en œuvre de l'EEDS en Italie: les pièces manquantes du cadre réglementaire existant en matière de santé numérique*, in N. DE GROVE VALDEYRON (sous la direction de), *op. cit.*, 2025.

– *Salute digitale nell'Unione Europea: tra innovazione ed equo accesso all'assistenza sanitaria*, in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Giappichelli, Torino, 2023.

FORGÓ N., HÄNOLD S., SCHÜTZE B., *The Principle of Purpose Limitation and Big Data*, in M. CORRALS, M. FENWICK, N. FORGÓ, *New Technology, Big Data and the Law*, Springer, Singapore, 2017.

GARBEN S., *Article 168 TFEU*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit.*, 2019.

–, *Articles 179-190*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit.*, 2019.

GAJA G., HAY P., ROTUNDA R.D., *Instruments for Legal Integration in the European Community – A Review*, in M. CAPPELLETTI, M. SECCOMBE, J.H. WEILER (eds.), *Integration Techniques and Judicial Process*, De Gruyter, Berlin, 1986.

GIANNITI L., MATROIANNI R., *Il ruolo dei parlamenti nazionali*, in F. BASSANINI, G. TIBERI (a cura di), *Le nuove istituzioni europee. Commento al Trattato di Lisbona*, Il Mulino, Bologna, 2008.

GORMLEY L., *Free Movement of Goods and Pre-emption of State Power*, in A. ARNULL, C. BARNARD (eds.), *A Constitutional Order of States? Essays in EU Law in Honour of Alan Dashwood*, Bloomsbury Publishing, London, 2011.

–, *The Internal Market: History and Evolution*, in N.N. SHUIBHNE (ed.), *Regulating the Internal Market*, Edward Elgar, Cheltenham, 2006.

GOVAERE I., *Internal Market Dynamics: On Moving Targets, Shifting Contextual Factors and the Untapped Potential of Article 3(3) TEU*, in I. GOVAERE, S. GARBEN (eds.), *op. cit*., 2020.

HAFEN E., *Personal Data Cooperatives. A New Data Governance Framework for Data Donations and Precision Health*, in J. KRUTZINNA, L. FLORIDI (eds.), *The Ethics of Medical Data Donation*, Springer, Cham, 2019.

HEIL H., *Directive 95/46/EC of the European Parliament and the Council*, in A. BÜLLESBACH, Y. POULLET, C. PRINS (eds.), *Concise European IT Law*, Kluwer Law International, Alphen aan den Rijn, 2010.

HENSELER S., TAMÒ-LARRIEUX A., *Reaching Beyond Its Territory – An Analysis of the Extraterritorial Scope of European Data Protection*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit.*, 2022.

HERVEY T., *The European Union and the Governance of Health Care*, in G. DE BÚRCA, J. SCOTT, (eds.), *Law and New Governance in the EU and the US*, Hart Publishing, Oxford, 2006.

–, *The Right to Health in European Union Law*, in T. HERVEY, J. KENNER (eds.), *Economic and Social Rights under the EU Charter of Fundamental Rights – A Legal Perspective*, Hart Publishing, Oxford-Portland, 2003.

HERVEY T., MCHALE J., *The Right to Health Care*, in S. PEERS et al. (eds.), *The EU Charter of Fundamental Rights. A Commentary*, Hart Publishing, Oxford, 2022.

–, *Data Protection and Health Information Privacy*, in T. HERVEY, J. MCHALE, *Health Law and the European Union*, CUP, Cambridge, 2004.

HUGHES K., *The Social Value of Privacy, the Value of Privacy to Society and Human Rights Discourse*, in B. ROESSLER, D. MOKROSINSKA (eds.), *Social Dimensions of Privacy: Interdisciplinary Perspectives*, CUP, Cambridge, 2015.

HUSTINX P., *EU Data Protection Law: The Review of Directive 95/46/EC and the*

Proposed General Data Protection Regulation, in M. CREMONA (ed.), *New Technologies and EU Law*, OUP, Oxford, 2017.

IRTI C., *Personal Data, Non-Personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. SENIGAGLIA, C. IRTI, A. BERNES (eds.), *Privacy and Data Protection in Software Service*, Springer, Singapore, 2022.

KAYE J., PRICTOR M., *Consent*, in G. LAURIE et al. (eds.), *Health Research Regulation*, CUP, Cambridge, 2021.

KELLERBAUER M., *Articles 114-118*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit.*, 2019.

KLAMERT M., *Articles 15-16*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019.

–, *Article 48*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019.

KOSTA V., *Fundamental Rights Mainstreaming in the EU*, in F. IPPOLITO, M.E. BARTOLONI, M. CONDINANZI, *op. cit*., Routledge, 2019.

KOSTAKOPOULOU D., *The Area of Freedom, Security and Justice and the European Union's Constitutional Dialogue*, in C. BARNARD (ed.), *The Fundamentals of EU Law Revised: Assessing the Impact of the Constitutional Debate*, OUP, Oxford, 2009.

KRANENBORG H., *Article 8 – Protection of Personal Data*, in S. PEERS et al. (eds.), *op. cit.*, 2022.

LARSEN L.B., *Some Reflections on Mutual Recognition in the Area of Freedom, Security and Justice*, in P. CARDONNEL, A. ROSAS, N. WAHL (eds.), *Constitutionalising the EU Judicial System: Essays in Honour of Pernilla Lindh*, Hart Publishing, Oxford, 2012.

LENAERTS K., *The EU Charter of Fundamental Rights: Scope of Application and Methods of Interpretation*, in V. KRONENBERGER, M.T. D'ALESSIO, V. PLACCO (sous la direction de), *De Rome à Lisbonne: les juridictions de l'Union européenne à la croisée des chemins: mélanges en l'honneur de Paolo Mengozzi*, Bruxelles, 2013.

LOCK T., *Articles 6-19*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019.

–, *Articles 35-38*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *op. cit*., 2019.

–, *Articles 51-54*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (eds.), *Commentary on the EU: Treaties and the Charter of Fundamental Rights*, OUP, Oxford, 2019.

LÖRCHER K., *Social Competences*, in N. BRUUN, K. LÖRCHER, I. SCHÖMANN (eds.), *The Lisbon Treaty and Social Europe*, Hart Publishing, Oxford, 2012.

LUCARELLI A., *Art. 35 Protezione della salute*, in R. BIFULCO, M. CARTABIA, A. CELOTTO (eds.), *L'Europa dei diritti. Commento alla carta dei diritti fondamentali dell'Unione europea*, Il Mulino, Bologna, 2001.

MALETIĆ I., *Derogations from the Regulation of Free Movement: Article 114 TFUE*, in P. KOUTRAKOS, J. SNELL (eds.), *Research Handbook on the Law of the EU's Internal Market*, Edward Elgar, Cheltenham, 2017.

MAMMARELLA G., *Storia d'Europa dal 1945 a oggi*, GLF Editori Laterza, Roma, 2006.

MANTELERO A., *Consultazione preventiva*, in R. D'ORAZIO et al., *Codice della privacy e data protection*, Giuffrè, Milano, 2021.

MANZINI P., *Antitrust e privacy: la strana coppia*, in P. MANZINI (a cura di), *I confini dell'antitrust. Diseguaglianze sociali, diritti individuali e concorrenza*, Giappichelli, Torino, 2023.

–, *La portata dei diritti garantiti dalla Carta dell'Unione europea: problemi interpretativi*

posti dall'art. 52, in L.S. ROSSI (a cura di), *Carta dei diritti fondamentali e Costituzione dell'Unione europea*, Giuffrè, Milano, 2002.

MARLETTA M., *Commento all'art. 168 TFUE*, in A. TIZZANO (a cura di), *op. cit.*, 2014.

MASTROIANNI R., *Le competenze dell'Unione*, in G. MORBIDELLI, F. DONATI (a cura di), *Una Costituzione per l'Unione europea*, Giappichelli, Torino, 2006.

MAYER SCHÖNBERG V., *Generational Development of Data protection in Europe*, in P.E. AGREE., M. ROTENBERG (eds.), *Technology and Privacy: The New Landscape*, The MIT Press, New York, 1997.

MENGOZZI P., *Commento all'articolo 12 TUE*, in A. TIZZANO (a cura di), *op. cit.*, Giuffrè, Milano, 2014.

MÍŠEK J., *Data Protection as Performance-Based Regulation*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022.

MIGLIAZZA M., *Art. 168. Sanità pubblica*, in F. POCAR, M.C. BARUFFI, A. ADINOLFI (a cura di), *op. cit.*, 2014.

MORI P., *Art. 296*, in A. TIZZANO (a cura di), *op. cit.*, 2014.

NAPOLETANO N., *L'evoluzione della tutela dei diritti fondamentali nell'Unione europea*, in A. CALIGURI, G. CATALDI, N. NAPOLETANO (a cura di), *La tutela dei diritti umani in Europa: tra sovranità statale e ordinamenti sovranazionali*, Cedam, Padova, 2010.

NASCIMBENE B., *L'iniziativa per una Conferenza sul futuro dell'Unione europea. Dalla "paura" all'"ambizione"*, in C. AMALFITANO, M. CONDINANZI, *Paura dell'Europa: spunti di razionalizzazione. Chi ha (ancora) paura dell'Europa?*, Giappichelli, Torino, 2020.

NAUDTS L., DEWITTE P., AUSLOOS J., *Meaningful Transparency through Data Rights: A Multidimensional Analysis*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022.

NIEMANN A., *Neofunctionalism*, in M. RIDDERVOLD, J. TRONDAL, A. NEWSOME (eds.), *The Palgrave Handbook of EU Crises*, Springer International Publishing, Cham, 2021.

ORLANDI M., *L'evoluzione del primato del diritto dell'Unione europea*, UTET Giuridica, Torino, 2012.

PALM W., GLINOS I.A., *Enabling Patient Mobility in the EU: Between Free Movement and Coordination*, in E. MOSSIALOS et al. (eds.), *Health Systems Governance in Europe: The Role of European Union Law and Policy*, CUP, Cambridge, 2010.

PASERI L., *Defining Scientific Research Within the EU's Politics of Data: The Impact on Personalized Smart Medicine*, in F. CASAROSA, F. GENNARI, A. ROSSI (eds.), *Enabling and Safeguarding Personalized Medicine*, Springer, Cham, 2025.

PERTICI A., *Dall'Europa dei mercati all'Europa dei diritti*, in G. RIVOSECCHI, M. ZUPPETTA (a cura di), *Governo dell'economia e diritti fondamentali dell'Unione europea*, Cacucci, Bari, 2010.

PETROČNIK T., *Secondary Use of Health Data in the EHDS: Public Interest and the Role of HDABs*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

PHILLIPS A.M., *The Right to Insert and Add Information to my Health Record – Does my Doctor Need to Know This? A Critical Discussion of the Right to Insert Information in an EHR Using the Example of Data from Direct-to-Consumer Genetic Testing*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

POLLICINO O., BASSINI M., *Art. 8 Carta dei diritti fondamentali dell'Unione europea*, in R. D'ORAZIO et al. (a cura di), *Codice della Privacy e Data Protection*, Giuffrè, Milano, 2021.

PRECHAL S., DE VRIES S., VAN EIJKEN H., *The Principle of Attributed Powers and the "Scope of EU Law"*, in L.F.M. BESSELINK, F. PENNINGS, S. PRECHAL (eds.), *The Eclipse of the Legality Principle in the European Union*, Kluwer Law, Alphen aan den Rijn, 2011.

PURTOVA N., *Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons*, in R. LEENES, N. PURTOVA, S. ADAMS (eds.), *Under Observation: The Interplay Between E-Health and Surveillance*, Springer, Berlin, 2017.

REICHEL J., *Administrative Tools for Balancing Social and Individual Interests. Data Protection Safeguards and Administrative Procedural Guarantees in Secondary Use in the European Health Data Space*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

–, *Allocation of Regulatory Responsibilities: Who Will Balance Individual Rights, the Public Interest and Biobank Research Under The GDPR?*, in S. SLOKENBERGA, O. TZORTZTATOU, J. REICHEL (eds.), *GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe*, Springer, Cham, 2021.

RENDA A., *Single Market 2.0: The European Union as a Platform*, in S. GARBEN, I. GOVAERE (eds.), *The Internal Market 2.0*, Hart Publishing, Oxford, 2020.

ROSSI L.S., *A New Revision of the EU Treaties After Lisbon?*, in L.S. ROSSI, F. CASOLARI, *op. cit*., 2010.

ROUVROY A., POULLET Y., *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy*, in S. GUTWIRTH et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009.

RINOLDI D.G., *Cercando Itaca: spazio europeo della salute, Next Generation EU e prospettive di approfondimento dell'integrazione continentale*, in V. SALVATORE (a cura di), *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Giappichelli, Torino, 2023.

SCHÜTZE R., *Limits to the Union's 'Internal Market' Competence(s): Constitutional Comparisons*, in L. AZOULAI (ed.), *op. cit.*, 2014.

SLEATH W., *The Role of National Parliaments in European Affairs*, in G. AMATO, H. BRIBOSIA, B. DE WITTE (eds.), *Genèse et destinée de la Constitution européenne: commentaire du traité établissons une Constitution pour l'Europe à la lumière des travaux préparatoires et perspectives d'avenir*, Bruylant, Brussels, 2007.

SLOKENBERGA S., *Setting the Foundations: Individual Rights, Public Interest, Scientific Research and Biobanking*, in S. SLOKENBERGA, O. TZORTZATOU, J. REICHEL (eds.), *op. cit.*, 2021.

SNELL J., *The Internal Market and the Philosophies of Market Integration*, in C. BARNARD, S. PEERS, *European Union Law*, OUP, Oxford, 2020.

SPANCER J.R., CSURI A., *EU Criminal Law*, in C. BARNARD, S. PEERS, *European Union Law*, OUP, Oxford, 2020.

SPAJIĆ D., *Transforming the Secondary Use of Patient Data in the European Health Data Space: A Challenge for the Patient's Right to Medical Confidentiality?*, in S. SLOKENBERGA, K.Ó. CATHAOIR, M. SHABANI (eds.), *op. cit.*, 2025.

STREINZ T., *The Evolution of European Data Law*, in P. CRAIG, G. DE BÚRCA (eds.), *The Evolution of EU Law*, OUP, Oxford, 2021.

STROZZI G., *Il sistema integrato di tutela dei diritti fondamentali dopo Lisbona: attualità e prospettive*, in L.F. PACE (a cura di), *Nuove tendenze del diritto dell'Unione europea dopo il Trattato di Lisbona*, Giuffrè, Milano, 2012.

SZYSZCZAK E., *Modernising Healthcare: Pilgrimage for the Holy Grail?*, in M. KRAJEWSKI, U. NEERGARD, J.W. VAN DE GRONDEN (eds.), *The Challenging Legal Framework for Services of General Interest in Europe. Between Competition and Solidarity*, TMC Asser Press, The Hague, 2009.

TOEBES B., *Right to Health and Health Care*, in D.P. FORSYTHE, *Encyclopaedia of Human Rights*, OUP, Oxford, 2009.

TREPTE S. et al., *Do People Know About Privacy and Data Protection Strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)*, in S. GUTWIRTH, R. LEENES, P. DE HERT (eds.), *op. cit*., 2014.

VANHERCKE B., *Europe 2020: Towards a More Social EU?*, in H. FRAZER et al. (eds.), *Europe 2020: Towards a More Social EU?*, Peter Lang, Bruxelles, 2010.

VILLANI U., *I principi di sussidiarietà e di proporzionalità nel diritto dell'Unione europea*, in L.F. PACE (a cura di), *op. cit.*, 2012.

VOGIATZOGLOU P., VALCKE P., *Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit.*, 2022.

WEATHERILL S., *The Fundamental Question of Minimum and Maximum Harmonisation*, in I. GOVAERE, S. GARBEN (eds.), *op. cit*., 2020.

–, *Maximum versus Minimum Harmonization: Choosing between Unity and Diversity in the Search for the Soul of the Internal Market*, in N.N. SHUIBHNE, L.W. GORMLEY (eds.), *From Single Market to Economic Union: Essays in Memory of John A. Usher*, OUP, Oxford, 2012.

–, *Competence and Legitimacy*, in C. BARNARD, O. ODUDU (eds.), *The Outer Limits of European Union Law*, Hart, Portland, 2009.

–, *Pre-emption, Harmonization and Distribution of Competence to Regulate the Internal Market*, in C. BARNARD, J. SCOTT (eds.), *The Law of the Single Market. Unpacking the Premises*, Bloomsbury Publishing, London, 2002.

WEIß W., *The Human Rights Regime Post Lisbon: Turning the CJEU into a Human Rights Court*, in S. MORANO-FOADI, L. VICKERS (eds.), *Fundamental Rights in the EU: A Matter for Two Courts*, Hart Publishing, Oxford-Portland, 2015.

WILSON G., *Comparative Legal Scholarship*, in M. MCCONVILLE, H.C. WING (eds.), *Research Methods for Law*, Edinburgh University Press, Edinburgh, 2017.

WISMAN T.H.A., TIJM R.J.L., *The Radical Reframing of the Purpose Limitation Principle – Why the Dutch Delegation Uprooted Data Protection*, in E. KOSTA, R. LEENES, I. KAMARA, *op. cit*., 2022.

WYATT D., *Community Competence to Regulate the Internal Market*, in M. DOUGAN, S. CURRIE (eds.), *50 Years of the European Treaties: Looking Back and Thinking Forward*, Hart Publishing, Oxford, 2009.

TZANOU M., *The GDPR and (Big) Health Data: Assessing the EU Legislator's Choices*, in M. TZANOU (eds.), *Health Data Privacy under the GDPR. Big Data Challenges and Regulatory Response*, Routledge, London and New York, 2021.

ZANFRIN-FORTUNA G., *Article 16 TFEU – Commentary*, in H-J.BLANKE, S. MANGIAMELI (eds.), *The Treaty on the Functioning of the European Union. A Commentary*, Springer, Berlin, 2021.

–, *Article 15. Right of Access by the Data Subject*, in C. KUNER et al. (eds.), *The EU General Data Protection Regulation – A Commentary*, OUP, Oxford, 2020.

–, *Forgetting about Consent. Why the Focus Should be on 'Suitable Safeguards*, in *Data Protection Law*, in S. GUTWIRTH, R. LEENES, P. DE HERT (eds.), *op. cit*., 2014.

ZILLER J., *Art. 51*, in R. MASTROIANNI, *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, Milano, 2017.

ARTICOLI SU RIVISTE

From Conference to Convention? Ideas and Prospects for a Reform of the EU Treaties, in *CMLRev.*, 2022, vol. 59.

ACETTO M., ZLEPTING S., *The Principle of Effectiveness: Rethinking Its Role in Community Law*, in *Eur. Pub. L.*, 2005, vol. 11.

ADAMSKI D., *Lost on the Digital Platform: Europe's Legal Travails with the Digital Single Market*, in *CMLRev*., 2018, vol. 55.

ADINOLFI A., *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE*, 2023, n. 15.

AHMED Z. et al., *Artificial Intelligence with Multi-Factual Machine Learning Platform Development for Better Healthcare and Precision Medicine*, in *Database*, 2020.

ALEMANNO A., *The Legality of Omnibus Legislation Under EU Law: A Preliminary Analysis of Omnibus I Simplification Directive of CSRD and CSDD and its Legal Consequences on the EU Legal Order*, in *SSRN*, 2025.

– *The Omnibus Road to Constitutional Drift: How the Rise of Omnibus Legislation Undermines Procedural Integrity in the EU*, in *Verfassungsblog*, 2025.

AMALFITANO C., *Il futuro del rinvio pregiudiziale nell'architettura giurisdizionale dell'Unione europea*, in *DUE*, 2022, vol. 3-4.

ANGHEL V., JONES E., *Is Europe Really Forged Through Crisis? Pandemic EU and the Russia-Ukraine War*, in *J. Eur. Public Policy*, 2023, vol. 30, n. 4.

ARENA A., *Exercise of EU Competence and Pre-emption of Member States' Power in the Internal and External Sphere: Towards "Grand Unification"?*, in *Yearb. Eur. L.*, 2016, vol. 35, n. 1.

–, *The Doctrine of Union Pre-emption in the EU Internal Market: Between Sein and Sollen*, in *Colum. J. Eur. L.*, 2010, vol. 17.

AUSLOOS J., MAHIEU R., VEALE M., *Getting Data Subject Rights Right. A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance*, in *JIPITEC*, 2020, vol. 10.

AZOULAI L., *The "Retained Powers" Formula in the Case Law of the European Court of Justice: EU Law as Total Law?*, in *Eur. J. Leg. Stud*., 2011, vol. 4, n. 2.

BARENTS R., *The Internal Market Unlimited: Some Observations on the Legal Basis of Community Legislation*, in *CMLRev.*, 1993, vol. 30, n. 1.

BERNIER A. et al., *Reconciling the Biomedical Data Commons and the GDPR: Three Lessons From the EUCAN ELSI Collaboratory*, in *Eur. J. Hum. Genet*., 2023, vol. 32, n. 1.

BAROCAS S., SELBST A.D., *Big Data's Disparate Impact*, in *Cal. Law Rev*., 2016, vol. 104.

BARTOLINI C., SIRY L., *The Right to be Forgotten in the Light of the Consent of the Data Subject*, in *Comput. Law Secur. Rev.*, 2016, vol. 32.

BECKER R. et al., *Purpose Definition as a Crucial Step for Determining the Legal Basis under the GDPR: Implications for Scientific Research*, in *JLB*, 2024.

–, *Secondary Use of Personal Health Data: When Is It "Further Processing" Under the GDPR, and What Are the Implications for Data Controllers*, in *Eur. J. Health Law*, 2023, vol. 30.

BELORTAJA B., *Less is More: The Redundant Application of Articles 6(1) and 9(1)(2) GDPR in* Krankenversicherung Nordrhein *(C-667/21)*, in *EU Law Live*, 2024.

BENNET S.C., *Right to Be Forgotten: Reconciling EU and US Perspectives*, in *Berkeley J. Int. L*, 2012, vol. 30.

BESTAGNO F., *La tutela della salute tra competenze dell'Unione europea e degli Stati membri*, in *SIE*, 2017, vol. 2.

BINCOLETTO G., *The EDPB-EDPS Joint Opinion on the Commission Proposal for a Regulation on the European Health Data Space: Key Issues to be Considered in the Legislative Process*, in *Eur. Data Protection L. Rev.*, 2022, vol. 3.

BINCOLETTO G., GUARDA P., *A Proactive GDPR-Compliant Solution for Fostering Medical Scientific Research as a Secondary Use of Personal Health Data*, in *Opinio Juris in Comparatione*, 2021, vol. 1.

BIRGIT W. et al., *Putting the GDPR into Practice: Difficulties and Uncertainties Experienced in the Conduct of Big Data Health Research*, in *Eur. Data Prot. L. Rev.*, 2021, vol. 7.

BOCONG Y., JIANNAN L., *The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation*, in *Int. J. Environ. Res. Public Health*, 2019, vol. 16, n. 6.

BOIN A., HART P., MCCONNELL A., *Crisis Exploitation: Political and Policy Impacts of Framing Contests*, in *J. Eur. Public Policy*, 2009, vol. 16.

BOSI G., *Expanding EU Competence in Health? The Need for and Feasibility of Treaty Change*, in *EU Law Live*, 2022.

BUCHER A., *Does Europe Need a Health Union?*, in *Policy Contribution*, 2022, n. 2.

BUITELAAR J.C., *Privacy: Back to the Roots*, in *Ger. Law J.*, 2012, vol. 13, n. 3.

BURLEY A.M., MATTLI W., *Europe before the Court: A Political Theory of Legal Integration*, in *International Organization*, 1993, vol. 47, n. 1.

BUSBY H., HERVEY T., MOHR A., *Ethical EU Law? The Influence of the European Group on Ethics in Science and New Technologies*, in *Eur. Law Rev.*, 2008, vol. 33.

BRAVO F., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, vol. 2.

–, *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf.*, 2023, vol. 3.

BRITO BASTOS F., PALKA P., *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity*, in *ECLR*, 2023, n. 3.

BRKAN M., *The Unstoppable Expansion of the EU Fundamental Right to Data Protection. Little Shop of Horrors?*, in *MJ*, 2016, vol. 23, n. 5.

–, *Data Protection and Conflict-of-Laws: A Challenging Relationship*, in *Eur. Data Prot. L. Rev.*, 2016, vol. 2.

BROOKS E. et al., *EU Health Policy in the Aftermath of COVID-19: Neofunctionalism and Crisis-Driven Integration*, in *J. Eur. Public Policy*, 2023, vol. 30, n. 4.

BROOKS E., GEYER R., *The Development of EU Health Policy and the Covid-19 Pandemic: Trends and Implications*, in *J. Eur. Integr.*, 2020, vol. 42, n. 8.

BROTHERS K.B., ROTHSTEIN M.A., *Ethical, Legal and Social Implications of Incorporating Personalized Medicine into Healthcare*, in *Future Med.*, 2014, vol. 15,

CABRAL P., *Cross-Border Medical Care in the European Union – Bringing Down a First Wall*, in *Eur. Law Rev*., 1999, vol. 24, n. 4.

CAGGIANO G., *La proposta di* Digital Service Act *per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post di AISDUE*, 2021, vol. 3.

CAPPELLETTI M., *Is the European Court of Justice Running Wild?*, in *Eur. Law Rev.*, 1987, vol. 12.

CARBINI P., *La Corte di giustizia si pronuncia sulla legittimità delle misure restrittive della libertà di circolazione durante il Covid-19*, in *Eurojus*, 2023.

CARRIÈRE-SWALLOW Y., HAKSAR V.*, International Monetary Fund; Issuing Body. The Economics and Implications of Data: An Integrated Perspective*, in *IMF*, 2019.

CASAROSA F., GENNARI F., *Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS*, in *EJRR*, 2025.

CASOLARI F., *A Constitutionally Oriented Reading of the EU Artificial Intelligence Act*, in *Science, Technology and Law – Mutual Impact and Current Challenges*, 2024.

CASOLARI F., *La tutela dei valori dell'Unione europea e le prerogative sovrane degli Stati membri: quali limitazioni?*, in *Unione europea e diritti*, 2025, n. 3.

–, *Il Processo di europeizzazione delle identità nazionali degli Stati membri: riflessioni sulle traiettorie del costituzionalismo europeo*, in *Quaderni AISDUE*, fasc. 1, 2024.

–, *The EU Approach towards Disaster Management. A Critical Appraisal in the Light of the Action Put in Place to Face the COVID-19 Pandemic*, in *YIDL*, 2023, vol. 4, n. 1.

–, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revised*, in *Eur. Foreign Aff. Rev.*, 2023, vol. 28, n. 4.

CASOLARI F., BUTTABONI C., FLORIDI L., *The EU Data Act in Context: A Legal Assessment*, in *Int. J. Law Inf. Technol*., 2024, vol. 20.

CANNATACI J.A., MIFSUD-BONNICI J.P., *Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty*, in *ICT*, 2015, vol. 14.

CELESTE C., *The Thin Border Between Individual and Collective Ethics: The Downside of GDPR*, in *The Lancet Oncology*, 2021, vol. 22, n. 1.

CELESTE E., *Digital Constitutionalism: A New Systematic Theorisation*, in *Int. Rev. Law, Comput. Technol*., 2019, vol. 33, n. 1.

CERVERA DE LA CRUZ P., LALOVA-SPINKS T., SHABANI M., *The European Health Data Space: An Opportunity to Strengthen Citizens Rights and Engage Citizens in Health Data Governance*, in *Front. Med.*, 2026.

CHIEFFI L., *Equità nella salute e nei servizi sanitari tra politiche europee e interventi statali*, in *Corti Supreme*, 2022, vol. 1.

–, *Una nuova stagione per i diritti sociali? La spinta offerta dal Recovery Fund per il rilancio dei welfare sanitari*, in *BioLaw Journal*, 2021, n. 4.

CIANCI L., *Dichiarazione europea sui diritti e principi digitali: quid pluris?*, in *DPCE*, 2022.

CIMINA V., *The Proposal for a European Health Data Space: Between Pursued Objectives and Data Protection Challenges*, in *ERA Forum*, 2023, vol. 24.

CISOTTA R., *Principi giurisprudenziali e nuove iniziative della Commissione in materia di patient mobility nell'Unione europea: un piccolo (o grande?) terremoto è in atto*, in *SIE*, 2007, vol. 3.

CLEMENS T., BRAND H., *Will COVID-19 Lead to a Major Change of the EU Public*

Health Mandate? A Renewed Approach to EU's Role Is Needed, in *Eur. J. Public Health*, 2020, vol. 30.

CLEMENS T., MICHELSEN K., BRAND H., *Supporting Health Systems in Europe: Added Value of EU Actions?*, in *Health Economics, Policy and Law*, 2014, vol. 9, n. 1.

COHEN J.E., *Irrational Privacy?*, in *J. Telecomm. & High Tech. L.*, 2012, vol. 10.

COMANDÉ G., *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 2019, vol. 1.

–, *Ricerca in sanità e data protection un puzzle…risolvibile*, in *Rivista italiana di medicina legale*, 2019, fasc. 1.

COMANDÉ G., SCHNEIDER G., *It's Time Leveraging the GDPR to Shift the Balance Towards Research-Friendly EU Data Spaces*, in *CMLRev.*, 2022, vol. 59.

–, *Differential Data Protection Regimes in Data-driven Research: Why the GDPR is More Research-friendly Than You Think*, in *Ger. Law J.*, 2022, vol. 23, n. 4.

–, *Can the GDPR Make Data Flow for Research Easier? Yes it Can, By Differentiating*, in *Comput. Law Secur. Rev.*, 2021, vol. 41.

CONTALDI G., *L'approccio regolatorio dell'Unione europea in materia di intelligenza artificiale*, in *Quaderni AISDUE*, 2026.

–, *Il significato attuale dell'economia sociale di mercato nell'ordinamento dell'Unione europea,* in *Ordine internazionale e diritti umani,* 2018, n. 5.

COSTA-CABRAL F., LYNKSEY O., *Family Ties: the Intersection between Data Protection and Competition in EU law*, in *CMLRev*., 2017, vol. 54, n. 1.

COSTA L., POULLET Y., *Privacy and the Regulation of 2012*, in *Comput. Law Secur. Rev.*, 2012, vol. 28.

CRAIG P., *The ECJ and the Ultra Vires Actions: a Conceptual Analysis*, in *CMLRev*., 2011, vol. 48, n. 2.

CROSS E., *Pre-emption of Member State Law in the European Economic Community: A Framework for Analysis*, in *CMLRev*., 1992, vol. 29, n. 3.

CURREN L., KAYE J., *Revoking Consent: a "Blind Spot" in Data Protection Law?*, in *Comput. Law Secur. Rev.*, 2010, vol. 26.

D'AMICO A., *The Boundary between EU Competition Law and the GDPR after* Meta, in *CMLRev*., 2024, vol. 61, n. 3.

DALLA CORTE L., *On Proportionality in the Data Protection Jurisprudence of the CJEU*, in *Int. Data Priv. Law*, 2022, vol. 12, n. 4.

–, *Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law*, in *EJLT*, 2019, vol. 10.

DAMJANOVIC D., *The EU Market Rules as Social Market Rules: Why the EU Can Be a Social Market Economy*, in *CMLRev*., 2013, vol. 50, n. 6.

DANIELE L., *Carta dei diritti fondamentali dell'Unione europea e Trattato di Lisbona*, in *DUE*, 2008, vol. 13.

DANIELE L., *La protezione dei diritti dell'uomo nell'Unione europea dopo il Trattato di Lisbona*, in *DUE*, 2009, vol. 3.

DAVESBE A., GUIGNER S., *La Communauté européenne de la santé (1952-1954). Une redécouverte intergouvernementaliste du projet fonctionnaliste de "pool blanc"*, in *Politique européenne*, 2013, vol. 3, n. 41.

DAWES A., *'Bonjour Herr Doctor': National Healthcare Systems, the Internal Market and Cross-Border Medical Care within the European Union*, in *Legal Issues of Economic Integration*, 2006, vol. 33, n. 2.
DAWSON M., *Better Regulation and the Future of EU Regulatory Law and Politics*, in *CMLRev*., 2016, vol. 53, n. 5.
DAVENPORT T., KALAKOTA R., *The Potential for Artificial Intelligence in Healthcare*, in *Future Healthc. J*., 2019, vol. 6, n. 2.
DAVIES G., *The European Union Legislature as an Agent of the European Court of Justice*, in *J. Common Mark. Stud*., 2016, vol. 54.
–, *Democracy and Legitimacy in the Shadow of Purposive Competence*, in *Eur. Law J*., 2015, vol. 21, n. 1.
–, *Subsidiarity: The Wrong Idea, in the Wrong Place, at the Wrong Time*, in *CMLRev*., 2006, vol. 43, n. 1.
–, *Welfare as a Service*, in *Legal Issues of Economic Integration*, 2002, vol. 29, n. 1.
DE ARMOND E.D., *To Cloack the Within: Protecting the Employees from Personality Testing*, in *DePaul Law Rev.*, 2012, vol. 61.
DE BELLIS S., *L'interazione fra parlamenti nazionali e le istituzioni comunitarie dopo Lisbona*, in *SIE*, 2010, vol. 3.
DE BÙRCA G., *After the Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?*, in *MJECL*, 2013, vol. 20, n. 2.
DE GREGORIO G., *The Rise of Digital Constitutionalism in the European Union*, in *Int. J. Const. Law*, 2021, vol. 19.
–, *Democratising Online Content Moderation: A Constitutional Framework*, in *Comput. Law Secur. Rev.*, 2019, vol. 36.
DE LA ROSA S., *The Directive on Cross-Border Healthcare or the Art of Codifying Complex Case Law*, in *CMLRev*., 2012, vol. 49, n. 1.
DELHOMME V., *The Legality of Covid-19 Travel Restrictions in an 'Area without Internal Frontiers': Court of Justice (Grand Chamber) 5 December 2023, Case C-128/22, Nordic Info*, in *Eur. Const. Law Rev.*, 2024, vol. 20, n. 2.
–, *Emancipating Health from Internal Market: For a Stronger EU (Legislative) Competence in Public Health*, in *Eur. J. Risk Regul*., 2020, vol. 11, fasc. 4.
DELHOMME V., HERVEY T., *The European Union's Response to the Covid-19 Crisis and (the Legitimacy of) the Union's Legal Order*, in *Yearb. Eur. L.*, 2022, vol. 41.
DELHOMME V., VAN OS C., *Building the European Health Union (2019-2024): Successes, Limits and Future Perspectives*, in *EJRR*, 2025, vol. 16, n. 3.
DEN EXTER A., SANTUARI A., SOKOL T., *One Year after the EU Patient Mobility Directive: A Three-Country Analysis*, in *Eur. Law Rev*., 2015, vol. 40, n. 2.
DE PASQUALE P., *Dalla flessibilità delle basi giuridiche alla normazione integrata: tecniche legislative funzionali alla rigidità del riparto di competenze nell'UE*, in *DUE*, 2025, vol. 1.
–, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *DUE*, 2022.
–, *L'economia sociale di mercato nell'Unione europea*, in *Studi sull'integrazione europea*, 2014, vol. 2.
DERMINE P., *The planning method: An inquiry into the constitutional ramifications of a new EU governance technique*, in *CMLRev*., 2024, vol. 61.

DE RUIJTER A., BROOKS E., *The European Health Union: Strengthening the EU's Health Powers?*, in *Eurohealth*, 2022, vol. 28, n. 3.
DE WITTE B., *The European Union's COVID-19 Recovery Plan: The Legal Engineering of an Economic Policy Shift*, in *CMLRev*., 2021, vol. 58, n. 3.
DE WITTE F., *EU Law, Politics, and the Social Question*, in *Ger. Law J.*, 2013, vol. 14, n. 5.
DI FEDERICO G., *From Dusk Till Dawn. The Case of F.T. v D.W. and the Right to Access Electronic Medical Records in Light of the Future European Health Data Space Regulation*, in *European papers*, 2024, vol. 9, n. 2.
–, *Principio di attribuzione e competenze esclusive degli Stati tra mito e realtà* (in corso di pubblicazione).
–, *Unione europea della salute, emergenze e professioni critiche: verso una disciplina ad hoc per gli operatori sanitari?*, in *Eurojus*, 2023, vol. 4.
–, *La direttiva 2011/24/UE e l'accesso alle prestazioni mediche nell'Unione europea, in Rivista di diritto della sicurezza sociale*, 2012, vol. 15, n. 3.
DI FEDERICO G., MARTINICO G., *Official Languages, National Identities and the Protection of Minorities: A Complex Legal Puzzle: Court of Justice (Grand Chamber) 7 September 2022, Case C-391/20, Boriss Cilevičs et al., ECLI:EU:C:2022:638*, in *Eur. Const. Law Rev.*, 2023, vol. 19, n. 2.
DOVE E.S., *The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era*, in *J. Law Med. Ethics*, 2018, vol. 46.
DOVE E.S., CHEN J.C., *Should Consent for Data Processing Be Privileged in Health Research? A Comparative Legal Analysis*, in *Int. Data Priv. Law*, 2020, vol. 10, n. 1.
DOCKSEY C., *Opinion 1/15: Privacy and Security, Finding the Balance*, in *Maastricht J. Eur. &Comp. L*., 2017, vol. 24.
DOUGAN M., *EU Competences in an Age of Complexity and Crisis: Challenges and Tensions in the System of Attributed Powers*, in *CMLRev.*, 2024, vol. 61, n. 1.
–, *Legal Developments*, in *JCMS*, 2010, vol. 48.
–, *Minimum Harmonization and the Internal Market*, in *CMLRev*., 2000, vol. 37.
DOUGLAS-SCOTT S., *The European Union and Human Rights after the Treaty of Lisbon*, in *HRLRev*., 2011, vol. 11, n. 4.
DUCATO R., *Data Protection, Scientific Research and the Role of Information*, in *Comput. Law Secur. Rev.*, 2020, vol. 37.
DUFF A., *Five Surgical Strikes on the Treaties of the European Union*, in *European Papers*, 2023, vol. 8, n. 1.
EIFERT M. et al., *Taming the Giants: The DMA/DSA Package*, in *CMLRev*., 2021, vol. 58, n. 4.
EISS R., *Confusion Over Data Privacy Law Stalls Scientific Progress*, in *Nature*, 2020.
ESTEVA A. et al., *A Guide to Deep Learning in Healthcare*, in *Nat. Med.*, 2019, vol. 25.
ERDOS D., *From the Scylla of Restriction to the Charybdis of Licence? Exploring the Scope of the "Special Purposes" Freedom of Expression Shield in European Data Protection*, in *CMLRev.*, 2015, vol. 52, n. 1.
EVANS B.J., *Much Ado About Data Ownership*, in *JOLT*, 2011, vol. 25.
FALKNER G. et al., *Digital Sovereignty – Rhetoric and reality*, in *JEPP*, 2024, vol. 31, n. 8.
FARHADI H., *Medical Internet of Things (m-IoT): Enabling Technologies and Emerging Applications*, in *IntechOpen*, 2019.
FAVILLI C., *Reciproca fiducia, mutuo riconoscimento e libertà di circolazione di rifugiati*

e richiedenti protezione internazionale nell'Unione europea, in *Rivista di diritto internazionale*, 2015, vol. 98, n. 3.
FERRARA F.M., KRIESI H., *Crisis Pressures and European Integration*, in *J. Eur. Public Policy*, 2022, vol. 29, n. 9.
FERRETTI F., *Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?*, in *CMLRev*., 2014, n. 3.
FERRI F., *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *DUE*, 2022, vol. 27, n. 2.
FINCK M., *Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy*, in *Eur. Law Rev.*, 2018, vol. 43, n. 1.
FINCK M., PALLAS F., *They Who Must not be Identified – Distinguishing Personal from Non-Personal Data under the GDPR*, in *Int. Data Priv. Law*, 2020, vol. 10, n. 1.
FINOCCHIARO G., *Intelligenza artificiale e responsabilità*, in *Contratto e impresa. Dialoghi con la giurisprudenza civile e commerciale*, 2020, vol. 2.
–, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it*., 2019.
–, *Introduzione al Regolamento europeo alla protezione dei dati*, in *Nuove leggi civ. comm*., 2017.
FINOCCHIARO G., GRECO L., *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, in *Diritto mercato tecnologia*, 2024.
FIORENTINI A., *Rethinking the Institutional Framework for the EU Data Regulations: Towards an Enhanced Administrative Integration*, in *REALaw*, vol. 13, n. 3, 2025.
–, *GDPR Meets Unfair Competition Law: The* Lindenapotheke *Ruling and Its Implications for Data Subjects and Controllers,* in *European Papers*, 2024, vol. 9, n. 3.
–, *Alla ricerca di un punto di equilibrio tra autonomia istituzionale ed effettività del diritto per le forme di integrazione amministrativa nel settore digitale*, in *Quaderni AISDUE, Sezione "Atti convegni AISDUE"*, 2023, n. 30.
–, *Il recepimento della Direttiva Open Data: un punto di svolta per la ricerca in Italia?*, in *Eurojus*, 2021.
FIORENTINI A., BULAND È., *The Day After the CoFoE (Act II): The EU Treaty Revision at the Mercy of Enlargement?*, in *Quaderni AISDUE*, 2024, fasc. 1.
–, *The Day After the CoFoE: Is the EU Ready for a Revision of the Treaty*, in *Quaderni AISDUE*, 2022, fasc. 1.
FIORILLO V., *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di giustizia dell'Unione europea*, in *federalismi.it*, 2017, n. 15.
FLOREA M., *Withdrawal of Consent for Processing Personal Data in Biomedical Research*, in *Int. Data Priv. Law*, 2023, vol. 13, n. 2.
FLORIDI L., *On Human Dignity as a Foundation for the Right to Privacy*, in *Philosophy & Technology*, 2016, vol. 29.
FRISCHHUT M., *The Missing Keystone of the 'European Health Union'. Historic Development, Status Quo (De Lege Lata) and Ideas De Lege Ferenda*, in *ZaöRV*, 2025, vol. 85.
FRONCZAK E., *Light on the Horizon for Transnational GDPR Enforcement: The EP Breathes Life into the Proposed Procedural Regulation*, in *Eu Law Live*, 2024.
–, *The Good, the Bad and the Ugly – A Take on the Commission Proposal for a GDPR Procedural Regulation*, in *Eu Law Live*, 2023.

GALETTA D.U., *Il principio di proporzionalità comunitario e il suo effetto spill over negli ordinamenti nazionali*, in *Nuove autonomie*, 2005.
GALIANO A. et al., *I dati non personali: la natura e il valore*, in *RIID*, 2020, n. 1.
GARBEN S., *From Sneaking to Striding: Combatting Competence Creep and Consolidating the EU Legislative Process*, in *Eur. Law J.*, 2020, vol. 26, nn. 5-6.
–, *Competence Creep Revised*, in *J. Common Mark. Stud*., 2019, vol. 57, n. 2.
–, *Constitutional (Im)balance between "the Market" and "the Social" in the European Union*, in *Eur. Const. Law Rev.*, 2017, n. 1.
GELLERT R., *Understanding the Notion of Risk in the General Data Protection Regulation*, in *Comput. Law Secur. Rev.*, 2018, vol. 34.
–, *We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection*, in *Eur. Data Prot. Law Rev*., 2016, vol. 2.
–, *Understanding Data Protection as Risk Regulation*, in *J. Internet Law*, 2015, vol. 18.
–, *Confronting the Competence Conundrum: Democratising the European Union through an Expansion of Its Legislative Powers*, in *Oxf. J. Leg. Stud.*, 2015, vol. 35, n. 1.
GELLERT R., GUTWIRTH S., *The Legal Construction of Privacy and Data Protection*, in *CLSR*, 2013, vol. 29.
GENOVESE S., *The European Health Data Space: A Step towards Digital and Integrated Care Systems*, in *J. Integr. Care*, 2022, vol. 30, n. 4.
GENTILE G., LYNSKEY O., *Deficient by Design? The Transnational Enforcement of the GDPR*, in *ICLQ*, 2022, vol. 71, n. 4.
GREZE B., *The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives*, in *Int. Data Priv. Law, 2019, vol. 9, n. 2.*
GIUDICI S., *Il Semestre europeo alla prova del coordinamento delle politiche sanitarie degli Stati membri: evoluzione e prospettive alla luce del Next Generation EU*, in *SIE*, 2022, vol. 3.
GOBBATO S., *Verso l'attuazione della direttiva (UE) 2019/1024 sul riutilizzo degli open data della PA: nuove opportunità per le imprese*, in *MediaLaws*, 2020, n. 2.
GONZÁLEZ FUSTER G., GELLERT R., *The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right*, in *IRLCT*, 2012, vol. 26.
GONZÁLEZ FUSTER G., GUTWIRTH S., *Opening up Personal Data Protection: A Conceptual Controversy*, in *Comput. Law Secur. Rev.*, 2013, vol. 29.
GENANNT DÖHMANN I.S., *A New Framework for Information Markets: Google Spain*, in *CMLRev.*, 2015, vol. 52, n. 4.
GRAEF I., GELLERT R., HUSOVEC M., *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation*, in *TILEC Discussion Paper No. 2018-029*, 2018.
GREENLEAF G., *The Influence of European Data Privacy Standards Outside Europe*, in *Int. Data Priv. Law*, 2012, vol. 2, n. 2.
GREER S.L., *Migration of Patients and Migration of Power: Politics and Policy Consequences of Patient Mobility in Europe*, in *Wis. Int'l L.J*., 2009, vol. 26, n. 3.
–, *Uninvited Europeanization: Neofunctionalism and the EU in Health Policy*, in *J. Eur. Public Policy*, 2006, vol. 13, n. 1.
GREER S.L., DE RUIJTER A., *EU Health Law and Policy in and After the COVID-19 Crisis*, in *Eur. J. Public Health*, 2020, vol. 30.

GREER S.L., RAUSHER S., *Destabilization Rights and Restabilization Politics: Policy and Political Reactions to European Union Healthcare Services Law*, in *J. Eur. Public Policy*, 2011, vol. 18.

GREER S.L., JARMAN H., BAERTEN R., *The New Political Economy of Health Care in the European Union: The Impact of Fiscal Governance*, in *Int. J. Health Serv*., 2016, vol. 46, n. 2.

GUY M., *Solidarity Rules? State Aid and Public Hospitals: Case C-492/21 P* Casa Apostolorum della Pia Società delle Figlie di San Paolo v. Commission, in *Eu Law Live*, 2023.

–, *Towards a European Health Union: What Role for Member States?*, in *Eur. J. Risk Regul*., 2020, vol. 11, n. 4.

HEIDEBRECHT S., *From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Market Governance*, in *JCMS*, 2024, vol. 62, n. 1.

HENDOLIN M., *Towards the European Health Data Space: From Diversity to a Common Framework*, in *Eurohealth*, 2021, vol. 27.

HERVEY T., *Community and National Competence in Health After Tobacco Advertising*, in *CMLRev*., 2011, vol. 38, n. 6.

HERVEY T., DE RUIJTER A., *The Dynamic Potential of European Union Health Law*, in *Eur. J. Risk Regul*., 2020, vol. 11, n. 4.

HERVEY T., MICHALAK M., *European Union Border Law During the COVID-19 Pandemic*, in *CMLRev*., 2025, vol. 62.

HIELKE H., *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, in *Eur. Data Protection L. Rev*., 2017, vol. 3.

HILDEN J., *Lobby in/Policy out? Assessing Lobbyist Influence on the GDPR*, in *Eur. Data Prot. L. Rev.*, 2021, vol. 7.

HOFMANN C.H., *Mapping the European Administrative Space*, in *West European Politics*, 2008, vol. 31, n. 4.

HOFMANN C.H., MUSTERT L., *Procedures Matter – What to Address in GDPR Reform and a New GDPR Procedural Regulation*, in *Eu Law Live*, 2023.

HOFFMANN S., *Obstinate or Obsolete? The Fate of the Nation-State and the Case of Western Europe*, in *Daedalus*, 1966, vol. 95, n. 3.

HOOGHE L., MARKS G., *Grand Theories of European Integration in the Twenty-First Century*, in *J. Eur. Public Policy*, 2019, vol. 26, n. 8.

HORGAN D. et al., *European Health Data Space – An Opportunity Now to Grasp the Future of Data-Driven Healthcare*, in *Healthcare*, 2022, vol. 10.

HORSLEY T., *Reflection on the Role of the Court of Justice as the "Motor" of European Integration: Legal Limits to Judicial Lawmaking*, in *CMLRev.*, 2013, vol. 50, n. 4.

HOWE III E.G., ELENBERG F., *Ethical Challenges Posed by Big Data*, in *Innov. Clin. Neurosci*., 2020, vol. 17, nn. 10-12.

IACOB N., SIMONELLI F., *Towards a European Health Data Ecosystem*, in *Eur. J. Risk Reg*., 2020, vol. 11.

IGLESIAS SANCHEZ S., *The Court and the Charter: The Impact of the Entry into Force of the Lisbon Treaty on the ECJ's Approach to Fundamental Rights*, in *CMLRev.*, 2012, vol. 49.

INGLESE M., *Il regolamento sull'intelligenza artificiale come atti per il completamento e il buon funzionamento del mercato interno?*, in *Quaderni AISDUE*, 2024, fasc. 2.

–, *Le prestazioni sanitarie transfrontaliere e la tutela della salute*, in *Diritto comunitario e degli scambi internazionali*, 2012, vol. 51.

JANCIC D., *The Barroso Initiative: Window Dressing or Democracy Boost?*, in *Utrecht L. Rev*., 2012, vol. 8.

JANS J.H., *Stop the Integration Principle?,* in *Fordham Int'L.J*., 2011, vol. 33.

KERTESZ F., *Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union*, in *EJHL*, 2024, vol. 31, n. 5.

KESSELHEIM A.S., MELLO M.M., *Confidentiality Laws and Secrecy in Medical Research: Improving Public Access to Data on Drug Safety*, in *Market Watch*, 2005, vol. 26, n. 2.

KISELEVA A., DE HERT P., *Creating a European Health Data Space. Obstacles in Four Key Legal Areas*, in *EPLR*, 2021, vol. 5.

KLAMERT M., *What We Talk About When We Talk About Harmonization*, in *Camb. Yearb. Eur. Leg. Stud*., 2015, vol. 17.

KOOPS B-J., *The Trouble with European Data Protection Law*, in *Tilburg Law School Legal Studies Research Paper Series*, 2014, vol. 4, n. 4.

–, *The Trouble with European Data Protection Law*, in *Int. Data Priv. Law*, 2014, vol. 4, n. 4.

KOKOTT J., SOBOTTA C., *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *Int. Data Priv. Law*, 2013, vol. 3.

KUCH P., *Teleology: The Missing Piece to Solving the GDPR Puzzle*, in *J. Data Prot. Priv.*, 2021, vol. 5, n. 1.

KUNER C., *International Agreements, Data Protection, and EU Fundamental Rights On The International Stage: Opinion 1/15, EU-Canada PNR*, in *CMLRev*., 2018, vol. 55.

–, *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15*, in *Verfassungsblog*, 2017.

–, *Data Protection Law and International Jurisdiction on the Internet*, in *Int. J. Law Inf. Technol.*, 2010, vol. 18, n. 2.

KRAJEWSKY M., *Providing Legal Clarity and Securing Policy Space for Public Services through a Legal Framework for Services of General Economic Interest: Squaring the Circle*, in *Eur. Public Law*, 2008, vol. 14, n. 3.

KRANENBORG H., *About Profiles, Profiling, Data Availability and AI: The Return of the Second Objective of the GDPR?*, in *EDPL*, 2025, vol. 1.

KŘEPELKA F., *Proposed Law for the European Health Data Space in Context*, in *Medicine, Law & Society*, 2023, vol. 16, n. 2.

KRUESZ C., ZOPF F., *The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU*, in *Eur. Data Protection L. Rev.*, 2021, vol. 7, n. 4.

KRUUS M., *Opting Out of Scientific Research with Health Data: The Limits of the EHDS and the GDPR*, in *EJHL*, 2025.

–, *The Public Interest Requirement in the Secondary Use of Health Data in Scientific Research: The Examples of Estonia and Finland*, in *Juridica International*, 2023, n. 32.

LACCHÈ L., *Agli albori dell'Europa libera e unita. Per gli ottant'anni del Manifesto di Ventotene (1941-2021)*, in *Quaderni costituzionali*, 2021, vol. 4.

LAZARO C., LE MÉTAYER D., *Control Over Personal Data: True Remedy or Fairy Tale?*, in *SCRIT-ed*, 2015, vol. 12, n. 1.

LAZZARONI M., *Le implicazioni istituzionali della pandemia da Covid-19: verso un'"Europa della salute"?*, in *SIE*, 2021, n. 2.

LEINO M., RUFFERT P., *Next Generation EU and its Constitutional Ramifications – A Critical Assessment*, in *CMLRev*., 2022, vol. 59.
LENAERTS K., LENAERTS K., *Constitutionalism and the Many Faces of Federalism*, in *The American Journal of Comparative Law*, 1990, vol. 38, n. 2.
–, *La vie après l'avis: Exploring the Principle of Mutual (Yet not Blind) Trust*, in *CMLRev*., 2017, vol. 54.
–, *The Principle of Mutual Recognition in the Area of Freedom, Security and Justice*, in *DUE*, 2015, fasc. 3.
–, *The Principle of Subsidiarity and the Environment in the European Union: Keeping the Balance of Federalism*, in *Fordham Int. Law J*., 1994, vol. 17, n. 4.
LODIE A., *Are Personal Data Always Personal? Case T-557/20 SRB v. EDPS or When the Qualification of Data Depends on Who Holds Them*, in *European Law Blog*, 2023.
LOUIS J-V., *National Parliaments and the Principle of Subsidiarity: Legal Options and Practical Limits*, in *Eur. Const. Law Rev.*, 2008, vol. 15.
LI W., *The Right to Data Portability in the European Health Data Space: A Follow-up*, in *Health&Aging Law Lab*, 2024.
LI W., QUINN P., *The European Health Data Space: An Expanded Right to Data Portability?*, in *Comput. Law Secur. Rev*., 2024, vol. 52.
LINDROOS-HOVINHEIMO S., *Op-Ed: The Principle of Openness Gives Way to Data Protection. Judgment in Case C-740/22 Endemol Shine*, in *Eu Law Live*, 2024.
–, *Who Controls our Data*? *The Legal Reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v. Jehovan todistajat*, in *Inf. Commun. Technol. Law*, 2019, vol. 28.
LINSKEY O., *Deconstructing Data Protection: The "Added-value" of a Right to Data Protection in the EU Legal Order*, in *Int. Comp. Law Q*, 2014, vol. 63.
MAIANI F., MIGLIORINI S., *One Principle to Rule Them All? Anatomy of Mutual Trust in the Law of the Area of Freedom, Security and Justice*, in *CMLRev*., 2020, vol. 57, n. 1.
MANIS M.L., *The Processing of Personal Data in the Context of Scientific Research. The New Regime under the EU-GDPR*, in *BioLaw Journal*, 2017, n. 3.
MANTELERO A., *The Future of Consumer Data Protection in the EU Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, in *Comput. Law Secur. Rev*., 2014, n. 6.
MANZELLA A., *Il Manifesto della Costituzione*, in *Quaderni costituzionali*, 2021, vol. 4.
MANZINI P., *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, in *I Post di AISDUE*, 2021, vol. 3.
MARELLI L. et al., *The European Health Data Space: Too Big To Succeed?*, in *Health Policy*, 2023.
MARELLI L., TESTA G., VAN HOYWEGHEN I., *Big Tech Platforms in Health Research: Re-Purposing Big Data Governance in Light of the General Data Protection Regulation's Research Exemption*, in *Big Data & Society*, 2021, vol. 8.
MARINES D., *Judicial Influence on Policy Outputs? The Political Constraints of Legal Integration in the European Union*, in *Comparative Political Studies*, 2015, vol. 48.
MARJANOVIC S. et al., *Understanding Value in Health Data Ecosystems*, in *Rand Health Quarterly*, 2018, vol. 7, n. 2.
MARTINES F., *La Conferenza sul futuro dell'Europa: uno strumento innovativo di*

partecipazione democratica per rafforzare la legittimità dell'Unione?, in *Annali AISDUE*, 2021, vol. 3.

MENGOZZI P., *The Judicial Protection of Individual Rights and the Principle of Proportionality after the Lisbon Treaty*, in *CYELS*, 2014, vol. 16.

MESZAROS J., HO C-H., *AI Research and Data Protection: Can the Same Rules Apply for Commercial and Academic Research under the GDPR?*, in *Comput. Law Secur. Rev.*, 2021, vol. 41.

MICCÙ R., *Questioni attuali intorno alla digitalizzazione dei servizi sanitari nella prospettiva multilivello*, in *federalismi.it*, 2021.

MIŠĆENIĆ E., HOFFMANN A-L., *The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)*, in *ECLIC*, 2020, n. 4.

MITSILEGAS V., *The Limits of Mutual Trust in Europe's Area of Freedom, Security and Justice: From Automatic Inter-State Cooperation to the Slow Emergence of the Individual*, in *Yearbook of European Law*, 2012, vol. 31, n. 1.

MOLNÁR-GÁBOR F. et al., *Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome Them by EU Measures: Insights from Germany, Greece, Latvia and Sweden*, in *Seminars in Cancer Biology*, 2022, vol. 84.

MOSTERT M. et al., *Big Data in Medical Research and EU Data Protection Law: Challenges to the Consent or Anonymise Approach*, in *Eur. J. Hum. Genet*, 2016, vol. 24.

MUIR E., *Drawing Positive Lessons From the Presence of 'The Social' Outside of EU Social Policy* Stricto Sensu, in *Eur. Const. Law Rev.*, 2018, vol. 14, n. 1.

MURPHY R.S., *Property Rights in Personal Information: An Economic Defense of Privacy*, in *Geo. L. J.*, 1996, vol. 84.

MUSTERT L., *Proceduralising GDPR Enforcement: How Complexity May Undermine Effective Cross-Border Data Protection*, in *Eur. Data Prot. L. Rev.*, 2025, vol. 11, n. 4.

–, *The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?*, in *Eur. Data Prot. L. Rev.*, 2023, vol. 9, n. 4.

NASCIMBENE B., *Il mercato unico digitale è una nuova frontiera dell'integrazione europea*, in *Eurojus*, 2025, fasc. 3.

–, *Il Mercato Unico Digitale quale nuova frontiera dell'integrazione europea. Considerazioni introduttive*, in F. ROSSI DAL POZZO, *Mercato Unico Digitale, dati personali e diritti fondamentali*, in *Eurojus*, 2019.

NEWDICK C., *The European Court of Justice, Trans-National Health Care and Social Citizenship – Accidental Death of a Concept?*, in *Wis. Int'l L.J.*, 2009, vol. 26.

NICOLAIDIS K., *Trusting the Poles? Constructing Europe through Mutual Recognition*, in *J. Eur. Public Policy*, 2007, vol. 14.

ÖBERG M-L., *The Legality of 'Covidfencing' Measures Under EU Free Movement Law:* Nordic Info BV v Belgische Staat, in *CMLRev*, 2025, vol. 62.

OLSEN J., *Towards a European Administrative Space?*, in *J. Eur. Public Policy*, 2003, vol. 10, n. 4.

OYER R.A. et al., *Increasing Racial and Ethnic Diversity in Cancer Clinical Trials: An American Society of Clinical Oncology and Association of Community Cancer Centres Joint Research Statement*, in *J. Clin. Oncol.*, 2022, vol. 40, n. 19.

PALMIERI S., GOFFIN T., *A Blanket That Leaves the Feet Cold: Exploring the AI Act Safety Framework for Medical AI*, in *Eur. J Health Law*, 2023, vol. 20.

PAPAKONSTANTINOU V., *The "Act-ification" of EU Law: The (Long-Overdue) Move Towards "Eponymous" EU Legislation*, in *European Law Blog*, 2021.

PAPAKONSTANTINOU V., DE HERT P., *The Regulation of Digital Technologies in the EU: The Law-Making Phenomena of 'Act-ification', 'GDPR Mimesis' and 'EU Law Brutality'*, in *TechReg*, 2022.

PARZIALE A., PULICE E., MASCALZONI D., *Mass-Scale G2B Data Sharing in an Emergency: Between the GDPR, Data Governance Act, and European Health Data Space*, in *European Journal of Health Law*, 2025, p. 30.

PEERS S., PRECHAL S., *Article 52 – Scope and interpretation of rights and principles*, in S. PEERS et al. (eds.), *op. cit.*, 2014.

PEETERS M., *Free Movement of Patients: Directive 2011/24 on the Application of Patients' Rights in Cross-Border Healthcare*, in *Eur. J. Health Law*, 2012, vol. 19, n. 1.

PELOQUIN D. et al., *Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data*, in *Eur. J. Hum. Genet*., 2020, vol. 28.

PHILIPPS M., KNOPPERS B.M., *Whose Commons? Data Protection as a Legal Limit of Open Science*, in *J. Law Med. Ethics*, 2019, vol. 47.

PISAPIA A., *La base giuridica per l'adozione degli atti dell'Unione*, in *SIE*, 2017, n. 3.

PISTOIA E., *Lo status del principio di mutua fiducia nell'ordinamento dell'Unione secondo la giurisprudenza della Corte di giustizia. Qual è l'intruso?*, in *FSJ*, 2017, n. 2.

PITRUZZELLA G., *Il costituzionalismo digitale tra Stati Uniti e Europa*, in *Unione europea e diritti*, 2025, fasc. 2.

POLLICINO O., *The Quadrangular Shape of the Geometry of Digital Power(s) and the Move Towards a Procedural Digital Constitutionalism*, in *Eur. Law J*., 2023, vol. 29, nn. 1-2.

–, *Di cosa parliamo quando parliamo di costituzionalismo digitale?*, in *Quaderni costituzionali*, 2023, fasc. 3.

–, *Judges, Privacy and Data Protection from a Multilevel Protection Perspective*, in *federalismi.it*, 2022, vol. 4.

PORCHIA O., *La sussidiarietà attraverso il riordino delle competenze? Il Trattato di riforma e la ripartizione delle competenze*, in *SIE*, 2010, vol. 3.

PORMEISTER K., *Genetic Research and Applicable Law: the Intra-EU Conflict of Laws as a Regulatory Challenge to Cross-border Genetic Research*, in *JLB*, 2018, vol. 5, n. 3.

–, *Genetic Data and the Research Exemption: Is the GDPR Going too Far?*, in *IDPL*, 2017, vol. 7.

POSNIK R., *Legal Considerations on the CJEU Judgment of 9 July 2020, C-272/19*, in *International Journal of Parliamentary Studies*, 2021, vol. 1.

POULLET Y., *Data Protection Legislation: What is at Stake for our Society and for Democracy?*, in *Comput. Law Secur. Rev.*, 2009, vol. 25.

POVSE D.F., *So Long and See you in the Next Pandemic? The Court's One-and-Done Approach on Permissible Reasons to Restrict Freedom of Movement for Public Health Reasons in the Nordic Info case (C-128/22) of 5 December 2023*, in *European Law Blog*, 2023.

PRECHAL S., *Mutual Trust before the Court of Justice of the European Union*, in *European Papers*, 2017, vol. 2.

PURNHAGEN K.P. et al., *More Competences than You Knew?: The Web of Health*

Competence for European Union Action in Response to the COVID-19 Outbreak, in *Eur. J. Risk Regul*., 2020, vol. 11, n. 2.

PURTOVA N., *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law Innov. Technol*, 2018, vol. 10, n. 1.

–, *The Illusion of Personal Data as no One's Property*, in *Law, Innov. Technol.*, 2015, vol. 7, n. 1.

–, *Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-Determination off the Table…and Back on Again?*, in *Comput. Law Secur. Rev.*, 2014, vol. 30, n. 1.

–, *Who Decides on the Future of Data Protection? Role of Law Firms in Shaping European Data Protection Regime*, in *Int. Rev. Law Comput*., 2014, vol. 28, n. 2.

PURTOVA N., LEENES R., *Code as Personal Data: Implications for Data Protection Law and Regulation of Algorithms*, in *Int. Data Priv. Law*, 2023, vol. 13, n. 4.

PETKOVA B., *Privacy as Europe's First Amendment*, in *Eur. Law J*., 2019, vol. 25, n. 2.

QUELLE C., *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-Based Approach*, in *Eur. J. Risk Reg.*, 2018, vol. 9.

QUINN E., *Much Ado About Nothing. The European Declaration on Digital Rights and Principles*, in *Verfassungsblog.de*, 2022.

QUINN P., *Research Under The GDPR – A Level Playing Field for Public and Private Sector Research*, in *Life Sci. Soc. Policy*, 2021, vol. 17.

–, *The Anonymisation of Research Data – A Pyric Victory for Privacy that Should Not Be Pushed Too Hard by the EU Data Protection Framework?*, in *EJHL*, 2017, vol. 24, n. 4.

QUINN P., DE HERT P., *The European Patients' Rights Directive: A Clarification and Codification of Individual Rights relating to Cross Border Healthcare and Novel Initiatives Aimed at Improving Pan-European Healthcare Cooperation*, in *Medical Law International*, 2012, vol. 12, n. 1.

QUINN P., QUINN L., *Big Genetic Data and its Big Data Protection Challenges*, in *Comput. Law Secur. Rev.*, 2018, vol. 34, n. 5.

QUINN P., ELLYNE E., YAO C., *Will the GDPR Restrain Health Data Access Bodies Under the European Health Data Space (EHDS)?*, in *Comput. Law Secur. Rev*., 2024, vol. 54.

RABESANDRATANA T., *European Data Law is Impeding Studies on Diabetes and Alzheimer's, Researchers Warn*, in *Science*, 2019.

RAPISARDA I., *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?*, in *Eur. dir. priv.*, 2021, fasc. 2.

RASPADORI F., *La Conferenza sul futuro dell'Europa e le colonne d'Ercole della lontananza dei cittadini*, in *BlogDUE*, 2022.

RENDA A., CASTRO R., *Towards Stronger EU Governance of Health Threats After the COVID-19 Pandemic*, in *Eur. J. Risk Regul*., 2020, vol. 11.

REGAN E., *The Role of the Principles of Mutual Trust and Mutual Recognition in EU Law,* in *DUE*, 2018, fasc. 2.

RIEDER C.M., *Cross-Border Movement of Patients in the EU: A Re-Appraisal*, in *Eur. J. Health Law*, 2017, vol. 24, n. 4.

RIGGIO G., *La parola ai cittadini: la Conferenza sul futuro dell'Europa*, in *Aggiornamenti sociali*, 2021, n. 5.

RIZCALLAH C., *The Principle of Mutual Trust and the Protection of Fundamental Rights in the Area of Freedom, Security and Justice: A Critical Look at the Court of Justice's Stone-by-Stone Approach*, in *MJECL*, 2023, vol. 30, n. 3.

RIZZO A., *La crisi pandemica e la nuova centralità delle politiche sanitarie europee alla luce della disciplina "EU4Health"*, in *SIE*, 2021, vol. 1.

ROSS M., *Effectiveness in the European Legal Order(s): Beyond Supremacy to Constitutional Proportionality?*, in *Eur. Law Rev.*, 2006, vol. 4.

ROSSI L.S., *Il principio del primato come "regola di coesione" dell'ordinamento dell'Unione europea*, in *Quaderni AISDUE*, 2024, fasc. 1.

–, ROSSI, *Fiducia reciproca e mandato d'arresto europeo. Il "salto nel buio" e la rete di protezione*, in *FSJ*, 2021, n. 1.

–, *Brevi osservazioni sulle recenti tendenze evolutive della giurisprudenza della Corte di Giustizia dell'Unione europea sulla protezione dei dati personali*, in *Eurojus,* 2020 Fascicolo speciale "Mercato unico digitale, dati personali e diritti fondamentali".

–, *Same Legal Value as the Treaties? Rank, Primacy, and Direct Effects of the EU Charter of Fundamental Rights*, in *Ger. Law J.*, 2017, vol. 18.

ROSSI DAL POZZO F., ANRÒ I., *Il Mercato Unico Digitale: tra antichi problemi e nuove sfide*, in *Eurojus*, 2025.

ROWLAND S. et al., *What is the Clinical Value of mHealth for Patients?*, in *Npj Digital Medicine*, 2020.

SALMONI F., *Diritti sociali e Unione europea. Dall'ordinamento comunitario allo stato sociale europeo*, in *Scritti in onore di G. Ferrara*, Torino, 2005.

SARTOR G., *Tutela della personalità e normativa per la "protezione dei dati". La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del "Datenschutz"*, in *Informatica e Diritto*, 1986, vol. 12.

SCHMITTER P.C., *Ernst B. Haas and the Legacy of Neofunctionalism*, in *J. Eur. Public Policy*, 2005, vol. 12, n. 2.

SCHNEIDER G., *Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence*, in *JIPITEC*, 2020, vol. 11.

SCHÖNBERGER D., *Artificial Intelligence in Healthcare: A Critical Analysis of the Legal and Ethical Implications*, in *Int. J. Law Inf. Technol*., 2019, vol. 27, n. 2.

SCHÜTZE R., *Supremacy without Pre-emption? The Very Slowly Emergent Doctrine of Pre-emption*, in *CMLRev*., 2006, vol. 43, n. 4.

SCHWARTZ P., *Property, Privacy, and Personal Data*, in *Harv. L. Rev.*, 2004, vol. 117, n. 7.

–, *Privacy and the Economics of Personal Health Care Information*, in *Tex. L. Rev*., 1997, vol. 76, n. 2.

SEITZ C., *The European Health Union and the Protection of Public Health in the European Union: Is the European Union Prepared for Future Cross-Border Health Threats?*, in *ERA Forum*, 2022, vol. 23.

SHABANI M., *Will the European Health Data Space Change Data Sharing Rules? Questions of Consent and Public Interest Research Loom Large*, in *Science*, 2022.

–, *The Data Governance Act and the EU's Move Towards Facilitating Data Sharing*, in *Molecular Systems Biology*, 2021, vol. 17, n. 3.

SHABANI M., YILMAZ S., *Lawfulness in Secondary Use of Health Data Interplay Between Three Regulatory Frameworks of GDPR, DGA & EHDS*, in *TechReg*, 2022.

SIMELL B.A. et al., *Transnational Access to Large Prospective Cohorts in Europe: Current Trends and Unmet Needs*, in *New Biotechnology*, 2019, vol. 49.
SIMITIS S., *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, in *Iowa L. Rev*., 1995, vol. 80.
SLOKENBERGA S., *Scientific Research Regime 2.0?, How the Proposed EHDS Regulation May Change the GDPR Research Regime*, in *TechReg*, 2022.
SOKOL T., *European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance*, in *EJHL*, 2024, vol. 4.
SOLA A., *Primi cenni di regolazione europea nell'economia dei dati*, in *MediaLaw*, 2022, vol. 3.
SOLOVE D.J., *Privacy Self-Management and the Consent Paradox*, in *Harv. Law Rev.*, 2013, vol. 126.
SØRENSEN K., *Brussels – We Have a Health Literacy Problem,* in *Eurohealth*, 2022, vol. 28, n. 3.
STARKBAUM J., FELT U., *Negotiating the Reuse of Health-data: Research, Big Data, and the European General Data Protection Regulation*, in *Big Data & Society*, 2019, vol. 6, n 2.
STAUNTON C. et al., *Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research*, in *Frontiers in Genetics*, 2022, vol. 13.
SVANTESSON D.J.B., *Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Sport Undermining the Regulation, in Int. Data Priv. Law*, 2015, vol. 5, n. 11.
STROBL J., CAVE E., WALLEY T., *Data Protection Legislation: Interpretation and Barriers to Research*, in *BMJ*, 2000, vol. 321.
SYRPIS P., *The Relationship between Primary and Secondary Law in the EU*, in *CMLRev*., 2015, vol. 52, n. 2.
SZYDŁO M., *How Should the EU Protect Personal Data without Undermining the Essential Functions of Member States and their Constitutional Principles?* Österreichische Datenschutzbehörde v. WK, in *CMLRev*, 2024, vol. 61 n. 5.
TAYLOR M.J., WHITTON T., *Public Interest, Health research and Data Protection Law: Establishing a Legitimate Trade-Off Between Individual Control and Research Access to Health Data*, in *Laws*, 2020, vol. 9, n. 1.
TENE O., POLONETSKY J., *Beyond IRBs: Ethical Guidelines of Data Research*, in *Wash. Lee Law Rev.*, 2016, vol. 72.
TERZIS P., *Compromises and Asymmetries in the European Health Data Space*, in *Eur. J. Health Law*, 2023, vol. 30.
TOPOL E., *High-Performance Medicine: The Convergence of Human and Artificial Intelligence*, in *Nat. Med.*, 2019, vol. 25.
TOSATO G.L., *Appunti in tema di economia sociale di mercato*, in *Scritti in onore di Giuseppe Tesauro*, 2014, vol. 2.
TOVO C., *I nuovi equilibri tra potere esecutivo e legislativo nell'Unione europea: l'accordo interistituzionale "Legiferare meglio"*, in *Eurojus*, 2016.
TOWNEND D., *Conclusion: Harmonization in Genomic and Health Data Sharing for Research: an Impossible Dream?*, in *Human Genetics*, 2018, vol. 137.
TOWNEND D. et al. (eds.), *The Data Protection Directive and Medical Research Across Europe*, Routledge, New York, 2004.
TREGGIANI E., *La complessa vicenda dei diritti sociali fondamentali nell'Unione europea*, in *SIE*, 2014, n. 1.

TRONDAL J., *Administrative Fusion: Less Than a European 'Mega-administration'*, in *J. Eur. Integr.*, 2009, vol. 31, n. 2.

TZANOU M., *Data Protection as a Fundamental Right Next to Privacy? Reconstructing' a not so New Right*, in *Int. Data Priv. Law*, 2013, vol. 3, n. 2.

–, *Balancing Fundamental Rights: United in Diversity? Some Reflections on the Recent Case Law of the European Court of Justice on Data Protection*, in *Croat. Yearb. Eur. Law & Policy*, 2010, vol. 6, n. 6.

TZANOU M., VOGIATZOGLOU P., *National Security and New Forms of Surveillance: From the Data Retention Saga to a Data Subject Centred Approach*, in *European Papers*, 2025, vol. 10, n. 3.

VANCHIERI C., *New EC Privacy Directive Worries European Epidemiologists*, in *J. Natl. Cancer Inst.*, 1993, vol. 83.

VAN DE GRONDEN J.W., VEENBRINK M., *EHDS and Free Movement of Patients: What EU Intervention is Needed?*, in *Eur. J. Health Law*, 2024.

VAN DIJK N., GELLERT R., ROMMETVEIT K., *A Risk to a Right? Beyond Data Protection Risk Assessments*, in *Comput. Law Secur. Rev.*, 2016, vol. 32.

VAN KESSEL R. et al*., The European Health Data Space Fails to Bridge Digital Divides*, in *BMJ*, 2022.

VAN VEEN E.B., *Observational Health Research in Europe: Understanding the General Data Protection Regulation and Underlying Debate*, in *Eur. J. Cancer*, 2018, vol. 104.

VAYENA E., *Value from Health Data: European Opportunity to Catalyse Progress in Digital Health*, in *The Lancet*, 2021.

VAYENA E., BLASIMME A., *Biomedical Big Data: New Models of Control Over Access, Use and Governance*, in *Bioethical Inquiry*, 2017, vol 14.

VERHENNEMAN G. et al., *How GDPR Enhances Transparency and Fosters Pseudonymisation in Academic Medical Research*, in *EJHL*, 2019, vol. 27, n. 1.

VILLANI U., *Il cammino europeo tra crisi e sviluppi*, in *SIE*, 2023, vol. 1.

–, *Metodo comunitario e metodo intergovernativo nell'attuale fase dell'Unione europea*, in *SIE*, 2019, vol. 2.

WACHTER S., MITTELSTADT B., *A Right to Reasonable Interferences: Re-thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Bus. Law Rev.*, 2019, vol. 2.

WAGNER J., BENECKE A., *National Legislation within the Framework of the GDPR, Limits and Opportunities of Member State Data Protection Law*, in *Eur. Data Prot. L. Rev.,* 2016, vol. 2, n. 3.

WARREN S., BRANDEIS L.D., *The Right to Privacy*, in *Harv. L. Rev.*, 1890, vol. 5.

WEATHERILL S., *The Limits of Legislative Harmonization Ten Years after* Tobacco Advertising*: How the Court's Case Law has become a "Drafting Guide"*, in *Ger. Law J.*, 2011.

WEILER J.H.H., *Vendesi cittadinanza. Commissione c. Malta: chi, davvero, smercia i valori europei*, in *QC*, 2024, vol. XLIV, n. 2.

WESTIN A., *Privacy and Freedom*, in *Wash. & Lee L. Rev*., 1968, vol. 25.

WILKINSON M. et al., *The FAIR Guiding Principles for Scientific Data Management and Stewardship*, in *Scientific Data*, 2016, vol. 3.

WOLF S., *The Proposed Patients' Rights Directive and the Reform of (Cross-Border) Healthcare in the European Union*, in *Leg. Issues Econ. Integr.*, 2009, vol. 35, n. 2.

WOUTERS B. et al., *Putting the GDPR into Practice: Difficulties and Uncertainties Experienced in the Conduct of Big Data Health Research*, in *Eur. Data Prot. L. Rev.*, 2021, vol. 7.

ZANFIR-FORTUNA G., *Follow the (Personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package*, in *EDPS at 20 Anniversary Volume* (in corso di pubblicazione).

ZAPOTOCZNA Z., *The European Union's Influence on the Organisation of National Healthcare Systems. Navigating the Trends after the Covid-19 Pandemic*, in *EJHL*, 2025, vol. 32.

ZELGER B., *The Right to Be Forgotten in the European Union: Towards a Uniform Approach*, in *GPLR*, 2022, vol. 3, n. 1.

ZILLER J., *Les Fabuleux Destins Des Explications Relatives à la Charte Des Droits Fondamentaux de l'Union Européenne*, in *Chemins d'Europe: Mélanges en l'honneur de Jean-Paul Jacqué*, 2010.

ZWICK D., DHOLAKIA N., *Contrasting European and American Approaches to Privacy in Electronic Markets: Property Right versus Civil Right*, in *Electronic Markets*, 2001, vol. 11.

ALTRI DOCUMENTI

Agenzia dell'Unione europea per i diritti fondamentali, *GDPR in Practice, Experiences of Data Protection Authorities*, 2024.

BARROSO J.M., *Political Guidelines for the Next Commission*, 2009.

BATURA O. et al., *The Emergence of Non-Personal Data Markets*, Publication for the Committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2023.

BEUC comments to Public consultation for legislative proposal on a European Health Data Space, Ref. Ares(2021)4878924, del 26 luglio 2021.

BOCCI M., *Veronesi e le quattro "p" della nuova medicina*, in *La Repubblica Firenze.it*, 2013.

BROUWER E., GERARD D. (eds.), *Mapping Mutual Trust: Understanding and Framing the Role of Mutual Trust in EU Law*, in *EUI Working Paper MWP*, 2016.

Centro di Coordinamento Nazionale dei Comitati Etici (CCNCE), Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale, 2023.

CNIL, *Délibération n 2023-083 du 20 juillet 2023 portant homologation d'une méthodologie de référence relative aux traitements de données de la base principale du Système national des données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissant dans le cadre de leurs intérêts légitimes (MR-008*).

–, *Délibération n 2023-082 du 20 juillet 2023 portant homologation d'une méthodologie de référence relative aux traitements de données de la base principale du Système national des données de santé mis en œuvre à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé par les organismes agissant dans le cadre de leur mission d'intérêt public (MR-007).*

–, *Délibération n 2023-002 du 12 janvier 2023 autorisant la société ELSAN SAS à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour*

finalité la constitution d'un entrepôt de données de santé, dénommé "EDS ELSAN". Demande d'autorisation n 2226980.
–, *Délibération n 2023-029 du 23 mars 2023 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur l'épidémiologie des maladies inflammatoires systémiques rares en France, intitulée "EMIR-Algo". Demande d'autorisation n 922278*.
–, *Délibération n 2023-028 du 23 mars 2023 autorisant l'Assistance publique – Hôpitaux de Paris à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur l'épidémiologie et les parcours de soins des enfants présentant des variations du développement génital, intitulée "VarGen". Demande d'autorisation n 922276*.
–, *Délibération n 2023-020 du 9 mars 2023 portant décision unique et autorisant la société "APM International" à mettre en œuvre des traitements automatisés à des fins de recherche, d'étude et d'évaluation dans le domaine de la santé nécessitant un accès aux données nationales du programme de médicalisation des systèmes d'information (PMSI). Saisine n 922297*.
–, *Délibération n 2023-042 du 27 avril 2023 autorisant la société Clinityx à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur la consommation en France de princeps et biosimilaires anti-TNF alpha, intitulée "Magellan Anti-TNF alpha". Demande d'autorisation n 923011.*
–, *Délibération n 2023-041 du 27 avril 2023 autorisant le Centre hospitalier universitaire de Poitiers et la société Clinityx à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalité une étude portant sur le taux de réintervention pour complication et le taux de réintervention pour récidive après implantation de bandelettes sous-urétrales au cours d'une chirurgie de l'incontinence urinaire d'effort en distinguant les deux voies d'abord, intitulée "Magellan Mesh". Demande d'autorisation n 922274.*
–, *Délibération n 2021-118 du 7 octobre 2021 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé.*

Consiglio d'Europa, Agenzia dell'Unione europea per i diritti fondamentali, Garante europeo per la protezione dei dati personali, *Manuale europeo in materia di protezione dei dati*, 2018.

Comitato europeo per la protezione dei dati personali, *Guidelines n. 01/2025 on Pesudonomisation*.
–, *Opinion n. 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models.*
–, *Statement n. 04/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR.*
–, *Guidelines n. 01/2024 on processing of personal data based on Article 6(1)(f)*.
–, *Contribution to the Report on the Application of the GDPR under Article 97*, 2023.
–, *Statement on enforcement cooperation*, 2022.
–, *Letter to the EU Commission on Procedural Aspects that Could be Harmonised at EU Level*, 2022.
–, Linee guida n. 02/2022 sull'applicazione dell'art. 60 del regolamento (UE) 2016/679.

–, Decisione vincolante n. 05/2022 relativa alla controversia sorta sul progetto di decisione dell'autorità di controllo irlandese concernente Meta Platforms Ireland Limited (Instagram) ai sensi dell'art. 65, par. 1, lett. a), regolamento (UE) 2016/679.
–, Parere n. 01/2022 sui diritti dell'interessato – diritto di accesso ai dati, versione 2.0.
–, *Guidelines on the Right of Access and Letter in Cookie Consent*, 2022.
–, Linee guida n. 10/2020 sulle limitazioni a norma dell'articolo 23 del regolamento (UE) 2016/679.
–, Linee guida n. 05/2020 sul consenso ai sensi del regolamento (UE) 2016/679.
–, Linee guida n. 05/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del regolamento (UE) 2016/679 (parte 1), versione 2.0.
–, Parere n. 03/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati.

Comitato e Garante europeo per la protezione dei dati personali, Parere congiunto n. 02/2026 sulla proposta di regolamento relativo alla semplificazione del quadro normativo in materia digitale (*Digital Omnibus*).
–, Parere congiunto n. 01/2025 sulla proposta di regolamento relativo alle misure di semplificazione per le PMI e le SMC, in particolare l'obbligo di conservazione dei dati ai sensi dell'articolo 30, par. 5, GDPR.
–, Parere congiunto n. 01/2023 sulla proposta di regolamento che stabilisce ulteriori norme procedurali del regolamento (UE) 2016/679.
–, Parere congiunto n. 03/2022 sulla proposta di regolamento sullo spazio europeo dei dati sanitari.
–, Parere congiunto n. 03/2021 sulla proposta di regolamento sulla governance dei dati.
–, Linee guida n. 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del regolamento (UE) 2016/679.
–, Linee guida n. 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19.

DG SANTE, *Frequently Asked Questions on the European Health Data Space*, 2025.
–, *Study Supporting the Impact Assessment of Policy Options for an EU Initiative on a European Health Data Space*, 2022.
–, *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, 2021.

eHealth Network, *Guideline on the Electronic Exchange of Health Data under Cross-Border Directive 2011/24/UE*, 2016.
–, *Guideline on Minimum/Nonexhaustive Patient Summary Dataset for Electronic Exchange in Accordance with the Cross-Border Directive 2011/24/UE*, 2013, aggiornate nel 2016.
–, *Guideline on ePrescriptions Dataset for Electronic Exchange under Cross-Border Directive 2011/24/UE*, 2014.

Response by ECOO to the European Health Data Space Consultation, Ref. Ares(2021)5516249, dell'8 settembre 2021.

DRAGHI M., *The Future of European Competitiveness. Part B. In-Depth Analysis and Recommendations*, 2024.

FABBRINI F., *The Conference on the Future of Europe A New Model to Reform the EU?*, in DCU Brexit Institute, Working Paper n. 12, 2019.

FAHY N. et al., *Use of Digital Health Tools in Europe Before, During and After COVID-19*, European Observatory on Health Systems and Policies, Copenhagen, 2021.

FOLEY P. et al., *Economic Value of Data Flows*, Publications Office of the European Union, Luxembourg, 2023.
Garante europeo per la protezione dei dati personali, *Study on the Secondary Use of Personal Data in the Context of Scientific Research*, Final Report EDPS/2019/02-04.
–, *Preliminary opinion n. 8/2020 on European Health Data Space*.
–, *A Preliminary Opinion on Data Protection and Scientific Research*, 2020.
–, *Study on the Appropriate Safeguards Under Article 89(1) GDPR for The Processing of Personal Data for Scientific Research*, 2019.
–, Parere n. 04/2015, Verso una nuova etica digitale. Dati, dignità e tecnologia.
–, *Opinion on the Communication from the Commission eHealth Action Plan 2012-2020-Innovative Healthcare for the 21st Century*, 2013.
–, Progetto di parere sulla proposta di direttiva del Parlamento europeo e del Consiglio concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (2009/C 128/03).
Garante italiano per la protezione dei dati personali, Parere sullo schema di decreto del Ministero della Salute sull'Ecosistema Dati Sanitari (EDS), ai sensi dell'art. 12, comma 15-*quater*, del decreto-legge 18 ottobre 2012, n. 179 (doc. web n. 10062302), del 26 settembre 2024.
–, Provvedimento del Garante per la protezione dei dati personali (doc. web n. 10016146), del 9 maggio 2024.
–, Provvedimento (doc. web n. 9948285), del 28 settembre 2023.
–, Provvedimenti (doc. web nn. 9752177, 9752221, 9752260, 9752299, 9752410, 752433, 9752490 e 9752524), del 24 febbraio 2022.
–, Parere al Ministero della Salute sullo schema di decreto, da adottare assieme al Ministro delegato per l'innovazione e la tecnologia digitale, di concerto con il Ministro dell'economia e delle finanze, sul FSE (doc. web n. 9802729), del 22 agosto 2022.
–, Parere al Ministero della Salute sullo schema di decreto, da adottare assieme al Ministro delegato per l'innovazione e la tecnologia digitale, di concerto con il Ministro dell'economia e delle finanze, sull'Ecosistema dei Dati Sanitari (doc. web n. 9802752), del 22 agosto 2022.
–, Parere n. 238 ai sensi dell'art. 110 del Codice della privacy e dell'art. 36 del Regolamento (doc. web. 9791886), del 30 giugno 2022.
–, Provvedimenti (doc. web nn. 9844989, 9845156, 9845312), del 15 dicembre 2022.
–, Parere alla Provincia autonoma di Trento su di uno schema di regolamento concernente la medicina di iniziativa del servizio sanitario provinciale (doc. web n. 9738538), del 16 dicembre 2021.
–, Parere alla Provincia autonoma di Trento su uno schema di regolamento concernente la medicina di iniziativa nel servizio sanitario provinciale (doc. web n. 9469372), del 1° ottobre 2020.
–, Parere sul disegno di legge provinciale concernente "Ulteriori misure di sostegno per le famiglie, i lavoratori e i settori economici connesse all'emergenza epidemiologica da COVID-19 e conseguente variazione al bilancio di previsione della Provincia autonoma di Trento per gli esercizi finanziari 2020-2022" (doc. web n. 9344635), dell'8 maggio 2020.
–, Prescrizioni relative al trattamento dei dati genetici, allegato n. 4 al provvedimento

recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 (doc. web n. 9124510), del 5 giugno 2019.
–, Prescrizioni relative al trattamento dei dati personali per scopi di ricerca scientifica, allegato n. 5 al provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 (doc. web n. 9124510), del 5 giugno 2019.
–, Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, d.lgs. 10 agosto 2018, n. 101 (provvedimento n. 515), del 19 dicembre 2018.
–, Linee guida in tema di FSE e di dossier sanitario (doc. web n. 1634116), 16 luglio 2009.
–, Prescrizioni in tema di FSE (doc. web n. 1633793), del 16 luglio 2009.

Gruppo di lavoro articolo 29 per la protezione dei dati, Linee guida del WP sul consenso ai sensi del regolamento (UE) 2016/679, WP 259.01, 2018.
–, Linee guida sulla trasparenza, WP 260 rev.01, 2018.
–, Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento (UE) 2016/679, WP 248 rev.01, 2017.
–, Linee guida sul diritto alla portabilità dei dati, WP 242, 2017.
–, Parere n. 06/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE.
–, Parere n. 03/2013 sulla limitazione delle finalità, WP 203.
–, Parere n. 15/2011 sulla definizione di consenso, WP 187.
–, Parere n. 03/2010 sul principio di responsabilità, WP173.
–, Parere n. 04/2007 sul concetto di dato personale, WP136.

Gruppo europeo sull'etica nella scienza e nelle nuove tecnologie, *Improving Pandemic Preparedness and Management – Lessons Learned and Ways Forward – Independent expert report*, 2020.
–, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, 2018.

Gruppo indipendente di esperti ad alto livello sull'Intelligenza Artificiale, Orientamenti etici per un'IA affidabile, 2019.

LETTA E., Much More Than a Market – Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for all EU Citizens, 2024.

LUPIÁÑEZ-VILLANUEVA F. et al., *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, 2021.

MARCUS J.S. et al., *The European Health Data Space*, Publication for the Committee on Industry, Research and Energy (ITRE), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2022.

OECD, *Health in the 21st Century. Putting Data to Work for Stronger Health Systems*, OECD Publishing, Parigi, 2019.
–, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Parigi, 2015.
–, *Empowering the Health Workforce Strategies to Make the Most of the Digital Revolution*, 2020.

SCOTT MARCUS J., PETROPOULOS G., YEUNG T., *Contribution to Growth: The European Digital Single Market. Delivering Economic Benefits for Citizens and Businesses*,

Study for the Committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2018.

WIEBE A., DIETRICH N., *Open Data Protection: Study on Legal Barriers to Open Data Sharing, Data Protection and PSI*, Universitätsverlag Göttingen, Göttingen, 2017.

WHO Regional Office for Europe, *Health and Care Workforce in Europe: Time to Act*, 2022.

–, *Digital Education for Building Health Workforce Capacity*, 2020.

Finito di stampare nel mese di aprile 2026
nella Stampatre s.r.l. di Torino
Via Bologna, 220

Studi di diritto dell'Unione europea

diretta da

A. Adinolfi, M. Condinanzi, P. Manzini, R. Mastroianni e F. Munari

---

Volumi pubblicati

1. Mauro Barbano, *EU State aid law as applied to the airline industry. Pandemic crisis and long-term perspectives*, 2025.
2. Nicole Lazzerini, *Le conseguenze giuridiche per le istituzioni dell'Unione europea dell'accertamento dell'illegittimità dei propri atti*, 2025.
3. Anna Fiorentini, *Lo spazio europeo dei dati sanitari. Nuovi equilibri costituzionali tra mercato unico digitale e Unione europea della salute*, 2026.