

Giorgia Bincoletto, Roberto Caso,
Paolo Guarda (a cura di)

I dati della sperimentazione clinica tra chiusura e apertura della conoscenza scientifica

Filosofia, politica, etica, diritto e prassi



I dati della sperimentazione clinica tra chiusura e apertura della conoscenza scientifica

***Filosofia, politica, etica,
diritto e prassi***

**A cura di
Giorgia Bincoletto, Roberto Caso, Paolo Guarda**

Ledizioni

Questo libro è pubblicato grazie al finanziamento dell'Università degli Studi di Trento, Facoltà di Giurisprudenza, Progetto PRIN 2022, *Clinical trial data between privatization of knowledge and Open Science* (CLIPKOS), codice progetto: 2022K4HBFA, CUP E53D23006760006

L'opera è rilasciata nei termini della licenza Creative Commons "Attribuzione – Condividi allo stesso modo 4.0 Internazionale (CC-BY-SA 4.0)" <https://creativecommons.org/licenses/by-sa/4.0/deed.it>.



I diritti d'autore sull'opera appartengono agli autori dei singoli contributi.

Le citazioni di altre opere sono riportate ai sensi degli art. 2, 21 e 33 Cost., 11 e 13 Carta dei diritti fondamentali dell'Unione Europea, nonché dell'art. 70 della l. 633/1941.

Giorgia Bincoletto, Roberto Caso, Paolo Guarda (a cura di), *I dati della sperimentazione clinica tra chiusura e apertura della conoscenza scientifica. Filosofia, politica, etica, diritto e prassi*
Prima edizione Ledizioni: giugno 2026

ISBN cartaceo: 9791256008292

ISBN versione ePub: 9791256008308

ISBN PDF Open Access: 9791256008315

In copertina: George Chalmers (1720-1791), *Portrait of James Lind (1716-1794)*, 1783, via Wikimedia Commons.

Il volume è acquistabile nelle versioni ePub e cartacee sul sito Internet www.ledizioni.it, nelle librerie online o tradizionali.

Il PDF Open Access è scaricabile da DOAB (Directory Open Access Books) o dal sito www.ledizioni.it

INDICE

Giorgia Bincoletto, Roberto Caso, Paolo Guarda	
Introduzione	11

PARTE I. FILOSOFIA, POLITICA ED ETICA DEI DATI

Maria Chiara Pievatolo	
Capitolo 1 – Di dati e di despoti: l'esclusiva sui dati clinici come epifania della "proprietà intellettuale"	23
1. <i>L'invasione degli ultra-PI: "pseudo-proprietà intellettuale" o "ultra-proprietà intellettuale"?</i>	24
2. <i>Alchimisti, califfi e mercanti: la parabola dell'ultra-PI</i>	30
3. <i>Di dati e di despoti</i>	36
4. <i>Anti-smottamento: diritto d'autore senza proprietà intellettuale</i>	44
Daniela Tafani	
Capitolo 2 – The imaginary patient. Fantastic health data and where to find them	49
1. <i>The radiologist and Wile E. Coyote</i>	50
2. <i>A conjectural paradigm</i>	52
3. <i>«But, Grandma, what big eyes you have!» «The better to treat you, my child»</i>	57
4. <i>Dissolving healthcare in AI slop</i>	65
Ivo De Gennaro	
Capitolo 3 – <i>Nulla animi labore</i> . Una nota sull'uso responsabile dell'intelligenza artificiale	81
1. <i>Introduzione</i>	82
2. <i>Goethe ovvero le espressioni offusanti</i>	84

3. <i>L'intelligenza nella prospettiva della scienza tecnizzata</i>	87
4. <i>L'intelligenza come tratto costitutivo dell'essere umano</i>	89
5. <i>La responsabilità etica</i>	92
6. <i>Leibniz ovvero la dignità e la servitù dell'intelligenza</i>	95
7. <i>Hegel ovvero la violenza del calcolo</i>	98
8. <i>Orientamenti per l'uso responsabile dell'AI</i>	99
9. <i>Conclusione</i>	104

Sergiusz Kazmierski

Capitolo 4 – Mapping fundamental problems of healthcare:

Plato on the possibility of Open Science and what we can learn from it	107
1. <i>Introduction</i>	107
2. <i>Three basic concepts of healthcare: science, the human being, and medicine</i>	110
3. <i>Factors and actors playing a key role in the production, use, and dissemination of medical data and the meaning of Open Science</i>	118
4. <i>Plato on the possibility of Open Science and what we can learn from it</i>	149

Ralf Lüfter

Capitolo 5 – «The good works in every thing,
but not everything that works is good».

Per una condivisione responsabile dei dati relativi agli studi clinici	157
1. <i>Introduzione</i>	158
2. <i>Tesi preliminari</i>	159
3. <i>Verso l'interroganza del bene</i>	177

Robert Simon

Capitolo 6 – Preliminari etici per il <i>data processing</i>	179
1. <i>L'oggetto della ricerca: il data processing e il concetto di strumento</i>	180
2. <i>Introduzione: La dimensione tecnica della relazione tra l'uomo e il mondo</i>	182
3. <i>Gli strumenti – L'organizzazione del mondo</i>	185
4. <i>Macchine – La macchinizzazione del mondo</i>	190
5. <i>Il Data Processor – La cibernetizzazione del mondo</i>	196
6. <i>Conclusione</i>	202

PARTE II

IL REGIME GIURIDICO DEI DATI DELLA SPERIMENTAZIONE CLINICA

Giorgia Bincoletto

Capitolo 7 – Tra apertura e chiusura. Un’analisi comparata sui ruoli delle <i>data exclusivity</i> e della <i>privacy</i> sulla riservatezza dei dati delle sperimentazioni cliniche farmacologiche	207
1. Le tensioni tra apertura e chiusura dei dati delle sperimentazioni cliniche	208
2. Le <i>data exclusivity</i> nel campo delle sperimentazioni cliniche	215
3. Un’analisi critica sulla natura e il ruolo delle <i>data exclusivity</i> : verso una maggiore apertura dei dati	235
4. Il ruolo della <i>privacy</i> sulla riservatezza dei dati clinici e le prospettive di apertura che tutelino i partecipanti	247
5. Conclusioni	256

Maurizio Borghi

Capitolo 8 – Il diritto alla trasparenza: segretezza commerciale e accesso ai dati degli studi clinici nell’Unione europea	259
1. Introduzione: il diritto alla salute e l’imperativo della trasparenza	260
2. Il percorso legislativo dalla divulgazione ‘reattiva’ a quella ‘proattiva’	266
3. Il quadro di divulgazione reattiva: il Regolamento 1049/2001 e la sua interpretazione giudiziale	268
4. La giurisprudenza sull’accesso ai dati degli studi clinici: dall’apertura a una (preoccupante) inversione di tendenza	273
5. Il ruolo formativo del Mediatore europeo nel modellare le politiche di accesso ai dati dell’EMA	276
6. L’Evoluzione delle politiche dell’EMA sulle informazioni commercialmente riservate (2007-2024)	282
7. Lo Spazio Europeo dei Dati Sanitari: un nuovo paradigma proattivo – ma per la trasparenza o per l’“innovazione”?	285
8. Conclusione e dubbi legittimi sull’impegno istituzionale alla trasparenza	289

Roberto Caso

Capitolo 9 – Monopoli farmaceutici e pseudo-proprietà intellettuale: l’esclusiva dei dati clinici nel diritto dell’Unione europea	293
1. Introduzione	294
2. Monopoli intellettuali e pseudo-proprietà intellettuale su informazioni e dati	295
3. L’esclusiva dei dati della sperimentazione preclinica e clinica: una pseudo-proprietà intellettuale	304

4. Alla ricerca di un bilanciamento tra esclusiva e trasparenza amministrativa: cenni all'esperienza dell'Unione europea	311
5. Conclusioni	321

Paolo Guarda

Capitolo 10 – “Lo strano caso del dottor Jekyll e del signor Hyde”, ovvero il segreto commerciale e l'European Health Data Space tra narrative e regole operazionali	323
1. Uso secondario dei dati e Spazio Europeo dei Dati Sanitari	324
2. Il segreto commerciale: tratti essenziali	329
3. Il Regolamento sullo Spazio Europeo dei Dati Sanitari alla prova del segreto commerciale	332
4. Doctor Jekyll (condivisione) e signor Hyde (chiusura): la disciplina europea sui dati tra narrative e realtà	336

Vitantonio Leuzzi

Capitolo 11 — Gli “usi commerciali sleali” nella “test data exclusivity”: le carenze di un modello economico controintuitivo	339
1. Introduzione	340
2. La dinamica dell'innovazione: due modelli a confronto	341
3. L'Art. 39(3) del TRIPS	351
4. “Usi commerciali sleali”: un'interpretazione adeguata	360
5. Conclusioni	367

Maria Francesca Del Buono

Capitolo 12 – Condivisione dei dati della sperimentazione clinica: obblighi normativi, governance e prassi a confronto tra Stati Uniti ed Unione europea	369
1. Introduzione	370
2. Spinte verso la trasparenza	372
3. Condivisione dei dati della sperimentazione clinica: modalità e nodi critici	379
4. Chi gioca la partita: dalla teoria alle policies aziendali	388
5. Chi vigila davvero: il ruolo centrale delle agenzie	397
6. Una possibile soluzione nel paradigma statunitense	401
7. Conclusioni	404

PARTE III
CHIUSURA E APERTURA DEI DATI DELLA SPERIMENTAZIONE CLINICA:
PRASSI E CASI STUDIO

Valentina Colcelli

Capitolo 13 – Banche dati, registri e studi basati su registri: una riflessione sull’apertura dei dati e sul ruolo dei Comitati Etici	409
1. <i>Introduzione: la fame dei dati per addestrare e validare efficacemente i modelli di IA, la centralità dei registri dei pazienti e dei Comitati Etici Territoriali</i>	410
2. <i>Il ruolo dei registri clinici nella ricerca farmacologica</i>	414
3. <i>La creazione di un registro e le modalità di apertura dei dati clinici: registri e studi basati su registri</i>	416
4. <i>Il ruolo dei Comitati Etici Territoriali nell’apertura dei dati dei registri dei pazienti</i>	420

Alessandra Langella, Antonio Lorito, Valentina Pagnanelli,
Valentina Colcelli, Laura Burzagli

Capitolo 14 – Cercando una governance aperta dei dati nella pratica clinica: il confronto tra le survey CLIPKOS e CCNCE (CET/CE)	423
1. <i>Introduzione</i>	424
2. <i>Fonti e campione e metodo di confronto</i>	430
3. <i>Focus sui dati aperti (Open Data) e trasparenza nella ricerca clinica</i>	436
4. <i>Conclusioni</i>	438

Andrea Barucci, Valentina Colcelli, Salvatore De Masi, Martina Falconi, Maria Carmela Leo, Antonio Marzola, Ilaria Romagnuolo, Carolina Sforzi, Roberto Pini

Capitolo 15 – Le sfide degli algoritmi opachi e della governance dei dati per i Comitati Etici Territoriali. Raccomandazioni per la redazione e valutazione di protocollo di studio	441
1. <i>Introduzione</i>	442
2. <i>Il ruolo dei Comitati Etici nella valutazione degli studi che impiegano IA</i>	444
3. <i>Ambito di applicazione</i>	446
4. <i>Le sfide poste dagli algoritmi opachi e dalla governance dei dati</i>	448
5. <i>Considerazioni in tema di applicazione dei sistemi di IA negli studi clinici</i>	451
6. <i>Aspetti etici e normativi dell’UE relativi all’IA nella ricerca clinica</i>	452
7. <i>Proposta di un metodo di valutazione per i Comitati Etici basato sulla fase di sviluppo dei sistemi di IA</i>	457
8. <i>La progettazione dello studio in base alle fasi di sviluppo del sistema di IA</i>	459

Roberto Caso	
Postfazione	465
Note biografiche	467

Paolo Guarda

CAPITOLO 10 – “LO STRANO CASO DEL DOTTOR JEKYLL E DEL SIGNOR HYDE”, OVVERO IL SEGRETO COMMERCIALE E L’EUROPEAN HEALTH DATA SPACE TRA NARRATIVE E REGOLE OPERAZIONALI

Abstract

Il capitolo indaga la complessa interazione tra il segreto commerciale e l’obiettivo di condivisione dei dati sancito dal Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS). Il Regolamento EHDS, entrato in vigore il 26 marzo 2025, è il primo “spazio di dati” settoriale dell’UE e mira a istituire un ecosistema per l’uso primario e secondario dei dati sanitari elettronici. Per promuovere l’uso secondario dei dati è cruciale bilanciare i benefici sociali con gli interessi degli innovatori privati e pubblici. Il segreto commerciale (disciplinato dalla Direttiva UE 2016/943) è un meccanismo di tutela che protegge informazioni segrete, con valore commerciale, sottoposte a misure ragionevoli di segretezza. L’articolo 52 del Regolamento EHDS è dedicato a questa intersezione, stabilendo che i dati sanitari qualificati come segreto commerciale debbano comunque essere resi disponibili per l’uso secondario e prevedendo la procedura di accesso. La soluzione ha sollevato diverse critiche da più fronti (dal possibile “over-claiming” da parte dei titolari dei diritti all’attribuzione di ampie responsabilità nella valutazione agli Organismi responsabili dell’accesso ai dati). L’EHDS si colloca nel quadro della “Strategia europea sui dati” (che include, tra gli altri, GDPR, DGA e DA), dove la polarizzazione tra la narrativa di “apertura” e la logica di “chiusura” del segreto commerciale si manifesta come il caso del “dottor Jekyll e signor Hyde” appunto. Nonostante il sovraccarico normativo generi confusione e rischi di frammentazione, l’approccio mirato degli spazi di dati è visto come un potenziale elemento positivo per definire regole operative più chiare.

This chapter investigates the complex interaction between trade secrets and the data-sharing objective established by the European Health Data Space Regulation (EHDS). The EHDS Regulation, which entered into force on March 26, 2025, is the first sector-specific “data space” of the EU and aims to establish an ecosystem for the primary and secondary use of electronic health data. To promote the secondary use of data, it is crucial to balance social benefits with the interests of private and public innovators. The trade secret (ruled by EU Directive 2016/943) is a protection mechanism that safeguards secret information, with commercial value, subject to reasonable secrecy measures. Article 52 of the EHDS Regulation is dedicated to this intersection, by establishing that health data qualified as a trade secret must still be made available for secondary use and setting out the procedure for accessing it. The solution has raised a series of criticisms from multiple sides (from the possible “over-claiming” by rights holders to the attribution of broad assessment responsibilities to the Health Data Access Bodies). The EHDS is situated within the framework of the “European Data Strategy” (which includes, among others, GDPR, DGA, and DA), where the polarization between the narrative of “openness” and the logic of “closure” of the trade secret manifests itself precisely as the case of “Doctor Jekyll and Mr. Hyde”. Despite the regulatory overload creating confusion and potential fragmentation, the targeted approach of specific data spaces is seen as a potential positive element for defining clearer operational rules.

1. Uso secondario dei dati e Spazio Europeo dei Dati Sanitari

L’Unione europea ha intrapreso un percorso che dovrebbe incentivare l’apertura e la condivisione del patrimonio informativo, proponendo un modello di governance dei dati alternativo a quello delle grandi piattaforme tecnologiche. Questo impegno si è concretizzato in un articolato corpo normativo – comprendente la Direttiva Open Data¹, il Data Gover-

1 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.

nance Act², il Data Act³, l’Artificial Intelligence Act⁴, etc. – coerente con gli obiettivi della “Strategia europea per i dati”⁵. Tale programma mira a istituire un mercato unico digitale che favorisca la circolazione dei dati tra imprese, ricercatori e istituzioni pubbliche. Per garantire un equilibrio tra innovazione e tutela, la Strategia si sviluppa su quattro pilastri fondamentali: i) adottare misure legislative in materia di governance, accesso e riutilizzo dei dati; ii) investire in dati, tecnologie digitali e competenze; iii) creare spazi di dati europei comuni in aree strategiche; e iv) dare potere alle imprese e ai cittadini europei⁶.

L’intero apparato normativo deve poi essere conforme alle discipline di ordine generale, anzitutto con quanto previsto dal 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 (Regolamento generale sulla protezione dei dati; di seguito: “GDPR”), il quale conferma il favor del legislatore europeo per il trattamento di dati a fini di

2 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, conosciuto come “Data Governance Act” o DGA). Si v. L. Specht-Riemenschneider, M. Hennemann (a cura di), *Data Governance Act. Article-by-Article Commentary*, Baden-Baden, Nomos, 2025.

3 Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio riguardante norme armonizzate sull’accesso equo ai dati e sul loro utilizzo (normativa sui dati, nota come “Data Act” - DA) del 13 dicembre 2023. Per approfondimenti si v. M. Hennemann, G.K. Ebner, B. Karsten, G. Lienemann, M. Wienroeder, *Data Act. An Introduction*, Baden-Baden, Nomos, 2024.

4 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull’intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull’intelligenza artificiale). Per approfondimenti sul suo contenuto si v., *ex plurimis*, C. Necati Pehlivan, N. Forgo, P. Valcke (a cura di), *The EU Artificial Intelligence (AI) Act*, Wolters Kluwer, 2025.

5 Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, Bruxelles, 19.2.2020, COM(2020) 66 final.

6 Cfr. C. Sganga, *Ventisei anni di direttiva database alla prova della nuova strategia europea per i dati: evoluzioni giurisprudenziali e percorsi di riforma*, in *Dir. inf.*, 2022, 3, 696.

ricerca, già previsto nella precedente Direttiva 95/46/CE⁷.

Il successo della strategia europea per la condivisione dei dati dipende dalla definizione di un quadro normativo improntato all'equità e alla chiarezza. In quest'ottica, l'Unione ha previsto la creazione di "spazi comuni di dati" interoperabili, di cui il Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari adottato l'11 febbraio 2025 (d'ora in avanti: Regolamento EHDS) rappresenta il primo modello settoriale. Tale Regolamento istituisce un ecosistema sanitario integrato, fondato su una governance condivisa, standard tecnici rigorosi e infrastrutture comuni. Sul piano individuale, l'EHDS mira a restituire ai cittadini il controllo effettivo sui propri dati sanitari elettronici, facilitandone l'accesso e la circolazione transfrontaliera. Parallelamente, si ambisce a consolidare un mercato unico per le cartelle cliniche elettroniche, i dispositivi medici e i sistemi di intelligenza artificiale ad alto rischio. Infine, il Regolamento introduce una disciplina organica per l'uso secondario dei dati, garantendo un accesso affidabile e sicuro per finalità di ricerca, innovazione e pianificazione delle politiche sanitarie.

L'EHDS non è in realtà uno spazio centralizzato per l'archiviazione dei dati, ma piuttosto una connessione "punto a punto" tra i titolari e gli utenti dei dati sanitari all'interno di un ambiente sicuro e incentrato sulla privacy per la messa in comune, l'accesso, la condivisione, l'elaborazione e l'utilizzo dei dati attraverso infrastrutture armonizzate.

A livello nazionale, l'EHDS deve essere interconnesso con i diversi ecosistemi di cartella clinica elettronica. Tuttavia, questo scenario è complicato a causa delle differenze tuttora presenti nelle normative interne in materia di protezione dei dati e nelle soluzioni tecniche e infrastrutturali. Prendendo ad esempio il contesto italiano, merita di essere menzionato il cosiddetto "Fascicolo Sanitario Elettronico" (FSE), che è stato recentemente sottoposto a restyling ed è ora denominato FSE versione 2.0⁸.

7 Cfr. P. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, Napoli, Edizioni Scientifiche Italiane, 2021, 134-172; R. Ducato, *Data protection, scientific research and the role of information*, in *Computer Law and Security Review*, 2020, 37, in Rete: <https://doi.org/10.1016/j.clsr.2020.105412>.

8 A seguito della riforma operata dal Decreto del Ministero della Salute 7 settembre 2023 (in attuazione dell'art. 12, co. 7, del D.L. 179/2012). Per una completa disamina sui sistemi di fascicolo sanitario elettronico e per una dettagliata descrizione di

Il Regolamento EHDS, entrato ufficialmente in vigore il 26 marzo 2025, delinea un percorso di attuazione progressivo caratterizzato da un esteso regime transitorio, necessario per garantire l’adeguamento dei sistemi sanitari nazionali. La tabella di marcia prevede che entro marzo 2027 vengano definiti gli atti di attuazione relativi alle specifiche tecniche fondamentali, concedendo agli stakeholder un ulteriore biennio, fino al marzo 2029, per l’effettiva implementazione tecnologica e la messa a norma dei sistemi. In tale data diverrà operativo lo scambio delle categorie prioritarie per l’uso primario, quali i profili sintetici dei pazienti e le prescrizioni elettroniche, contestualmente all’attivazione delle norme per la maggior parte dei dati per l’uso secondario. Una successiva estensione, prevista per il marzo 2031, includerà nel sistema di scambio anche la diagnostica per immagini, i referti di laboratorio e i documenti di dimissione ospedaliera, mentre l’apertura a paesi terzi e organizzazioni internazionali per scopi di uso secondario è posticipata al marzo 2035, sotto il vincolo di rigorose condizioni di sicurezza. Tale ecosistema, fondato su infrastrutture armonizzate, garantisce un ambiente sicuro e incentrato sulla privacy per la condivisione, l’elaborazione e l’utilizzo delle informazioni sanitarie.

Per quanto concerne l’uso secondario, l’articolo 51 individua le categorie minime di dati che devono essere messe a disposizione, la cui gestione è affidata agli Organismi per l’Accesso ai Dati Sanitari (Health Data Access Body - HDAB). L’iter procedurale prevede che i richiedenti inoltrino una domanda formale agli HDAB, ai sensi dell’articolo 67, ai fini del rilascio della necessaria autorizzazione prevista dall’articolo 68. In conformità ai principi di protezione dei dati, l’accesso è garantito prioritariamente in forma anonimizzata, ammettendo il trattamento di dati non anonimi solo qualora l’istanza dimostri puntualmente l’impossibilità di perseguire le finalità dichiarate tramite l’utilizzo di soli dati anonimizzati.

Un elemento centrale della disciplina è l’art. 53, che delimita le finalità ammesse per l’uso secondario dei dati sanitari. Gli organismi competenti (HDAB) possono autorizzare il trattamento solo se strettamente necessario per scopi specifici, tra cui spicca la ricerca scientifica (lett. e). Tale at-

alcuni modelli nazionali si v. G. Bincoletto, *Data Protection by Design in the E-Health Care Sector. Theoretical and Applied Perspectives*, Nomos, Baden-Baden, 2021, 229-283.

tività deve generare benefici per il settore pubblico o garantire standard elevati di sicurezza e qualità nelle cure e nei dispositivi medici. Rientrano in questo ambito anche l'innovazione di prodotto e l'addestramento di sistemi di Intelligenza Artificiale e algoritmi per la sanità digitale⁹.

A tutela della riservatezza, l'art. 71 introduce il diritto di opt-out, consentendo agli interessati di opporsi al trattamento dei propri dati per queste finalità. Questo meccanismo, assente nella bozza originaria e frutto di intensi negoziati in sede di trilogia, deve essere garantito dagli Stati membri con modalità semplici e reversibili.

L'esercizio dell'opt-out inibisce la disponibilità e il trattamento futuro del set di dati dell'interessato, senza tuttavia inficiare la validità delle attività di ricerca già autorizzate o avviate precedentemente alla revoca. Resta ferma la facoltà dei legislatori nazionali di prevedere deroghe specifiche: i dati "esclusi" potranno comunque essere resi disponibili qualora siano necessari a enti pubblici (nazionali o dell'Unione) per finalità imperative di salute pubblica. Infine, il Regolamento concede agli Stati la possibilità di innalzare il livello di tutela per categorie di dati particolarmente sensibili – come quelli genomici, epigenomici o provenienti da biobanche e app di benessere – consentendo l'introduzione di garanzie supplementari o il passaggio a un modello di opt-in (consenso espresso).

È un dato acquisito che i processi di innovazione, specialmente in ambito scientifico, producano un vasto patrimonio informativo che esula dalle tutele della proprietà intellettuale. Tale esclusione può dipendere dalla natura embrionale delle conoscenze, dall'assenza dei requisiti tecnici per la protezione o da scelte strategiche dei privati che preferiscono mantenere il riserbo per ragioni competitive. Per rendere effettivo il riutilizzo dei dati in ambito sanitario, è dunque essenziale bilanciare il progresso sociale con le aspettative degli innovatori. In tale ottica, la disciplina del segreto commerciale può rappresentare una questione fondamentale.

Il presente studio si propone di esplorare l'intersezione tra il Regolamento EHDS e il segreto commerciale, un profilo d'indagine ancora poco esplorato dalla dottrina, ma decisivo nel dibattito sullo spazio europeo dei dati sanitari.

9 Sul rapporto tra EHDS, disciplina in materia di protezione dei dati personali e impatto dei sistemi di intelligenza artificiale si v. I. Sanchez Frias, *Secondary uses of health data under the European Health Data Space. Connections with the GDPR and the impact of AI*, in *Revista General de Derecho Europeo*, 2025, 65, 212-223.

2. Il segreto commerciale: tratti essenziali

I processi creativi che caratterizzano la ricerca portano allo sviluppo di informazioni significative che possono non rientrare nell'ambito della protezione fornita dai tradizionali diritti di proprietà intellettuale ma che si ritiene, comunque, importante mantenere riservate. A tal proposito si parla allora di “segreto commerciale”, o anche di “segreto industriale”, “know-how proprietario” o ancora di “tecnologia proprietaria”.

Fino al 2016 non esistevano leggi armonizzate relative alla protezione dei segreti commerciali a livello dell'Unione europea. Come soluzione a tale disomogenea protezione, è stata emanata la Direttiva UE 2016/943 del Parlamento europeo e del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro la loro acquisizione, l'utilizzo e la divulgazione illeciti, con la finalità di armonizzare la disciplina europea garantendo un livello equivalente di protezione, introdurre una definizione uniforme del termine «segreto commerciale» e, infine, di fornire misure comuni contro l'acquisizione, l'utilizzo e la divulgazione illecita di segreti commerciali¹⁰.

Da una prospettiva più generale non si tratta di una vera e propria forma di proprietà sui dati, ma di una tutela di “quasi-privativa”, che permette di essere attivata nei confronti di chiunque (come un tradizionale

10 Per maggiori approfondimenti si v. T. Aplin, A. Radauer, M.A. Bader, N. Searle, *The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis*, in *IIC*, 2023, 54, 826-858; V. Piretti, *Big Data e segreto industriale: tra diritti, doveri e tutele*, in *diritto.it*, 2020, in Rete: <https://www.diritto.it/big-data-e-segredo-industriale-tra-diritti-doveri-e-tutele/>; V. Falce, *Ingegneria inversa e decompilazione come limiti alla tutela del segreto commerciale - Spunti sull'intima coerenza del codice della proprietà industriale*, in *Contr. e imp./Europa*, 2018, 36; V. Falce, *Dati e segreti. Dalle incertezze del regolamento Trade Secret ai chiarimenti delle linee guida della Commissione UE*, in *Dir. industriale*, 2018, 2, 155-159; S. Serafini, *Luci e ombre della nuova disciplina sul segreto commerciale*, in *Corriere giur.*, 2018, 11, 1329-1338; V. Falce, *Tecniche di protezione delle informazioni riservate - Dagli accordi Trips alla direttiva sul segreto industriale*, in *Riv. dir. ind.*, 2016, 1, 129-157; D. Arcidiacono, *The Trade Secrets Directive in the International Legal Framework*, in *European Papers*, 2016, vol. 1, n. 3, 1073-1085; C. Paschi, *La tutela delle informazioni riservate*, in C. Galli, A.M. Gambino (a cura di), *Codice commentato della proprietà industriale e intellettuale*, Torino, 2012, 909; M. Libertini, *Le informazioni aziendali segrete come oggetto di diritti di proprietà industriale*, in *Riv. it. per le scienze giuridiche*, 2011, 137-96.

diritto di esclusiva), con la peculiarità che non si applica a qualsiasi tipo di violazione, ma è subordinata al fatto che l'acquisizione sia avvenuta in "modo abusivo"¹¹. I rimedi possono includere il risarcimento del danno o provvedimenti di carattere inibitorio. La protezione può integrare di fatto gli altri diritti di proprietà intellettuale fintanto che le informazioni in questione non siano di dominio pubblico. Allo stesso tempo, la protezione del segreto è applicabile anche nei casi in cui non sussistono diritti di proprietà intellettuale, né possano esistere, a condizione che le informazioni siano mantenute segrete e gli altri requisiti per ottenere la protezione vengano soddisfatti¹².

Perché un'informazione sia considerata, e quindi protetta come, "segreto commerciale", essa deve integrare quanto previsto all'art. 2, pt. 1, della direttiva: a) essere segreta nel senso che l'informazione non è, nel suo insieme o nella precisa configurazione e combinazione con altri elementi, generalmente nota o facilmente accessibile a persone che normalmente si occupano del tipo di informazione in questione; b) avere un valore commerciale; c) essere stata sottoposta a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo è soggetta al fine di mantenerle segrete.

A differenza di quanto accade per la tutela brevettuale, ciò che viene tutelato dal segreto commerciale non deve essere nuovo. Inoltre, non è richiesta alcuna forma di registrazione. Pertanto, la protezione è tendenzialmente illimitata e gratuita. Per questi motivi, tale tutela può apparire

11 La natura di tale diritto, con riferimento al contesto italiano, è assai controversa. L'originaria formulazione nel Codice della proprietà industriale aveva portato alcuni a ritenere che si fossero concretizzati i contorni tipici di una tutela *erga omnes* dei segreti d'impresa, quale quella riconosciuta ai diritti di proprietà intellettuale non titolati. Questa tesi, però, contrastava con l'interesse costituzionalmente rilevante alla promozione dell'innovazione: rispetto, infatti, agli obblighi di trasparenza che gravano sul titolare del brevetto, ad esempio, nel caso di segreto commerciale non si determina alcuno stimolo all'innovazione futura e alla concorrenza tra gli inventori: cfr. L.C. Ubertazzi (a cura di), *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, VII ed., Padova, 2019, 608-610, in part. 609 e i riferimenti dottrinali ivi contenuti. Cfr. anche G. Resta, *Nuovi beni immateriali e numerus clausus dei diritti esclusivi*, in G. Resta (a cura di), *Diritti esclusivi e nuovi beni immateriali*, Bologna, 2010, 53-61.

12 Cfr. E. Derclaye, M. Leitner, *Intellectual Property Overlaps. A European Perspective*, Oxford-Portland, 2011, 21 ss., 172 ss., 223 ss.

particolarmente allettante ad alcuni attori del mercato dell’innovazione.

La direttiva definisce, inoltre, quali attività poste in essere senza il consenso del detentore siano da considerarsi acquisizione, utilizzo e divulgazione illecita di segreti commerciali (art. 4): ad esempio qualora siano avvenute mediante accesso non autorizzato, appropriazione o copia non autorizzate di documenti, oggetti, materiali, sostanze o file elettronici sottoposti al lecito controllo del detentore del segreto commerciale e che contengono il segreto commerciale stesso o dai quali esso può essere desunto (par. 2, lett. a)); oppure ponendo in essere qualsiasi altra condotta che, secondo le circostanze, è considerata contraria a leali pratiche commerciali (par. 2, lett. b)); o ancora in violazione di un accordo di riservatezza (par. 3, lett. b)), ecc. La responsabilità della violazione del segreto commerciale si estende anche a chi, al momento dell’acquisizione, utilizzo o divulgazione, fosse a conoscenza o, secondo le circostanze, avrebbe dovuto essere a conoscenza del fatto che il segreto era stato ottenuto direttamente o indirettamente da un terzo che illecitamente lo utilizzava o lo divulgava (par. 5).

La Direttiva sul segreto commerciale non è focalizzata esclusivamente sui “dati” in senso tecnico, ma istituisce un regime di protezione tecnologicamente neutrale applicabile a un «ampio spettro di know-how e informazioni commerciali» (Cons. 2)¹³. Nel contesto applicativo dell’EHDS, è difficile che un singolo dato isolato possieda un valore economico intrinseco tale da giustificare la protezione; è invece più probabile che tale requisito sia soddisfatto da set di dati aggregati, proprio come quelli soggetti agli obblighi di condivisione del Regolamento. Oltre al contenuto informativo, il valore commerciale può risiedere negli aspetti strutturali e metodologici: le tecniche di organizzazione e gestione dei database, i processi di archiviazione, etichettatura e tracciamento, nonché gli algo-

13 Nel contesto sanitario, ad esempio, il segreto commerciale viene invocato per la protezione delle informazioni farmaceutiche e delle sperimentazioni cliniche. Cfr. Aplin, Radauer, Bader, Searle, *The Role of EU Trade Secrets Law in the Data Economy*, cit., 828-829; A. Nordberg, *Trade secrets, big data and artificial intelligence*, in J. Schovsbo et al. (a cura di), *The harmonization and protection of trade secrets in the EU: an appraisal of the EU directive*, Edward Elgar, 194–220 (ch 11); J. Drexler, *Data access and control in the era of connected devices. Study on behalf of BEUC*, 2018, https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf.

ritmi proprietari impiegati per l'analisi dei dati raccolti¹⁴.

3. Il Regolamento sullo Spazio Europeo dei Dati Sanitari alla prova del segreto commerciale

I benefici sociali derivanti dalla ricerca in ambito medico e gli interessi degli innovatori del settore pubblico e privato per un sistema di proprietà intellettuale efficiente devono essere valutati congiuntamente. Una delle motivazioni dichiarate dei sistemi di proprietà intellettuale è il supporto all'innovazione. Pertanto, il modo in cui il Regolamento EHDS interagisce con tali sistemi rappresenta un aspetto fondamentale per garantire la corretta realizzazione dell'intero panorama europeo dell'innovazione.

La Direttiva sul segreto commerciale aveva già riconosciuto la necessità di trovare un bilanciamento tra l'interesse alla salute pubblica e le logiche di cui alla disciplina del segreto commerciale. Il Considerando 21 afferma:

«In linea con il principio di proporzionalità, le misure, le procedure e gli strumenti di tutela destinati a proteggere i segreti commerciali dovrebbero essere tarati in modo da raggiungere l'obiettivo di un corretto funzionamento del mercato interno per la ricerca e l'innovazione, in particolare dissuadendo dall'acquisizione, dall'utilizzo e dalla divulgazione illeciti di segreti commerciali. Tali misure, procedure e strumenti di tutela dovrebbero essere tarati in modo da non compromettere o minare i diritti, le libertà fondamentali e l'interesse pubblico, come la pubblica sicurezza, la tutela dei consumatori, la sanità pubblica e la

14 Questi rappresentano anche i requisiti per attivare la protezione del diritto d'autore in tale contesto: l'art. 3, Direttiva 96/9/CE del Parlamento europeo e del Consiglio dell'11 marzo 1996 sulla protezione giuridica delle banche dati, infatti, così recita: «le banche dati che, in ragione della selezione o disposizione dei loro contenuti, costituiscono una creazione intellettuale propria dell'autore sono protette come tali dal diritto d'autore». Per maggiori approfondimenti si v. P. Guarda, *Il regime giuridico dei dati della ricerca*, cit., 78-88. Come noto le banche dati, nel contesto europeo, sono oggetto di un altro (contestatissimo diritto): la Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati (Direttiva Banche Dati) attribuisce, infatti, al costituente della banca dati un diritto c.d. sui generis. Cfr. J.B. Hugenholtz, *Implementing the European Database Directive*, International Intellectual Property Law & Policy, 4, New York, USA, 2000.

protezione dell’ambiente, e non dovrebbero pregiudicare la mobilità dei lavoratori (...)».

Il Regolamento EHDS dedica l’art. 52 proprio a questa intersezione. L’assunto di partenza è che anche i dati sanitari qualificati come segreto commerciale (o protetti da diritti di proprietà intellettuale in generale) devono essere resi disponibili per l’uso secondario (par. 1). I “titolari dei dati”, poi, sono tenuti ad informare l’Organismo responsabile dell’accesso ai dati sanitari (Health Data Access Body - HDAB) circa la presenza di eventuali segreti commerciali nei set di dati che sarebbero tenuti a condividere ai sensi del Regolamento, giustificando la necessità di protezione (par. 2). L’HDAB prevede, allora, misure specifiche appropriate e proporzionate (giuridiche, organizzative e tecniche) necessarie per proteggere il segreto (par. 3). Si subordina, inoltre, l’accesso ai dati (autorizzazione) al rispetto di misure giuridiche, organizzative e tecniche (es. accordi contrattuali; clausole contrattuali tipo elaborate dalla Commissione) (par. 4). Infine, qualora l’accesso ai dati comporti un grave rischio per il segreto commerciale, l’HDAB lo nega (par. 5). Questo schema, come diremo in seguito, ha ricevuto critiche da più parti.

Quello del bilanciamento di così diversi interessi in gioco è aspetto comune e trasversale anche ad altri interventi normativi di cui all’European Data Strategy. Il Data Governance Act, ad esempio, che stabilisce i principi relativi all’accesso e al riutilizzo dei dati detenuti dagli enti pubblici ai fini del riutilizzo, all’art. 3, par. 1, lett. a), richiama «i dati detenuti dagli enti pubblici che sono protetti da (...) riservatezza commerciale, compresi i segreti aziendali, professionali e aziendali». Il termine «riservatezza commerciale» si riferisce anche ai dati protetti da segreti commerciali, know-how protetto e qualsiasi altra informazione la cui divulgazione indebita avrebbe un impatto sulla posizione di mercato o sulla salute finanziaria dell’impresa (Cons. 10)¹⁵. Il Data Act, inoltre, ha l’obiettivo di creare un sistema complesso di diritti di accesso, (ri)utilizzo e portabilità dei dati che mira a promuovere non solo lo sviluppo di nuovi e innovativi servizi correlati o prodotti connessi, ma anche a stimolare lo sviluppo di servizi aggiuntivi che utilizzano dati già raccolti da una va-

15 Cfr. L. Specht-Riemenschneider, *Article 3. Categories of data*, in L. Specht-Riemenschneider, M. Hennemann (a cura di), *Data Governance Act. Article-by-Article Commentary*, Baden-Baden, Nomos, 2025, 117, in part. 127-129.

rietà di servizi correlati o altrimenti connessi (tra cui l'Internet of Things (IoT))¹⁶. Il segreto commerciale svolge un ruolo nel garantire lo scambio di conoscenze tra imprese e istituti di ricerca all'interno e all'esterno del mercato interno. Il DA, allora, al Cons. 31 stabilisce che i titolari dei dati non possono, in linea di principio, rifiutare una richiesta di accesso ai dati esclusivamente sulla base del fatto che determinati dati siano considerati segreti¹⁷. Gli articoli 4, par. 6, e 5, par. 9, sviluppano lo stesso principio: quando si concede l'accesso agli utenti o si trasferiscono dati a terzi, gli eventuali segreti commerciali dovrebbero essere divulgati solo a condizione che vengano adottate tutte le misure necessarie per preservarne la riservatezza. In base a questo nuovo quadro, gli utenti potrebbero essere di fatto gravati da un obbligo di riservatezza in relazione ai dati che costituiscono la digitalizzazione dei propri comportamenti determinati dall'utilizzo di dispositivi IoT¹⁸. Da una prospettiva aziendale, questa regola potrebbe avere l'effetto collaterale di incentivare i titolari dei dati a invocare sistematicamente tale tutela in chiave difensiva o ad imporre all'utente misure di riservatezza particolarmente severe ed estese al fine di proteggere le proprie pratiche aziendali.

Tornando al Regolamento EHDS, le critiche sollevate alla previsione di cui all'art. 52 sono molteplici. Da un lato, si segnala il rischio di possibile "over-claiming" da parte dei titolari dei dati che, al fine di restringere l'accesso ai propri dataset, potrebbero richiedere in maniera esagerata l'attivazione della protezione. Dall'altro, gli stessi titolari di dati o gli innovatori privati criticano l'assetto dell'EHDS perché l'attribuzione di responsabilità così ampie agli HDAB, affinché agiscano da controllori nel valutare cosa costituisca informazione commercialmente riservata e debba quindi essere protetta come segreto commerciale, apparirebbe eccessivo rispetto alle specifiche competenze di cui potrebbero essere

16 Per maggiori approfondimenti si v. M. Hennemann, G.K. Ebner, B. Karsten, G. Lienemann, M. Wienroeder, *Data Act. An Introduction*, Baden-Baden, Nomos, 2024. Più in particolare con riferimento al contesto dell'IoT cfr. G. Noto la Diega, *Internet of Things and the Law. Legal strategies for consumer-centric smart technologies*, New York, Routledge, 2023.

17 Per un'analisi approfondita del rapporto tra DA e segreto commerciale, si v. E.D. Noyette, L. Stähler, T. Margoni, *Data Secrets: The Data Act's New Trade Secrets Framework*, in *IIC*, 2025, 56, 984–1014.

18 Cfr. Hennemann, Ebner, Karsten, Lienemann, Wienroeder, *Data Act. An Introduction*, cit., 109-110.

dotati questi organismi e, soprattutto, potrebbe portare a dissuadere i titolari di dati dall'avviare e proseguire le loro attività di ricerca nell'UE. Da più parti, infine, si chiede di rafforzare il coordinamento tra stakeholder pubblici e privati, sia nella creazione delle regole sia nella loro messa a terra¹⁹.

L'analisi suggerisce, dunque, che il modello delineato dall'EHDS non elimina la tensione tra apertura e protezione, ma la istituzionalizza, trasferendone la gestione a meccanismi procedurali e a valutazioni discrezionali degli organismi competenti.

Il segreto commerciale è stato, storicamente, uno strumento alternativo alla tradizionale proprietà intellettuale per il mondo «dato-centrico» essendo maggiormente flessibile e profilabile su diversi contesti applicativi²⁰. Se esso rappresenti un facilitatore o un ostacolo ai processi innovativi in generale è questione annosa e di non facile soluzione. Considerazioni e dubbi simili si possono sviluppare declinando la discussione nel contesto che qui ci impegna e portare a chiederci se esso sia veramente compatibile con aspettative e obiettivi di cui all'EHDS. Trattiamo in generale di protezioni che non sono caratterizzate dal tipico trade-off sociale delle privative in materia di proprietà intellettuale (protezione in cambio di descrizione dell'idea innovativa; protezione della modalità espressiva in cambio di libertà per le idee, ecc.). È, infatti, protezione che si applica a prescindere, senza scambio sociale, e molti ritengono che possa produrre risultati socialmente dannosi con l'effetto di avere innovazioni che non entrano mai nel pubblico dominio²¹. Le innovazioni tecnologiche e concettuali introdotte dall'Intelligenza Artificiale pongono ancora nuove sfide alla governance dei dati, rilanciando tensioni costanti e la ricerca di un equilibrio tra l'imperativo dell'apertura e gli interessi di mantenere chiusi i dati e le informazioni²².

19 Si v. gli argomenti proposti da *EFPIA position on the Regulation on the European Health Data Space (EHDS)*, in Rete: <<https://www.efpia.eu/media/2t2dem05/efpia-position-on-ehds.pdf>>.

20 Cfr. D. S. Levine, T. Sichelman, *Why Do Startups Use Trade Secrets?*, 94 *Notre Dame L. Rev.* 751, 758, 760 (2019).

21 Cfr. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, cit., 126.

22 Si v. Sanchez Frias, *Secondary uses of health data under the European Health Data Space*, cit., pp. 212-231 (in Rete: <<https://dialnet.unirioja.es/servlet/revista?codigo=5683>>).

4. Doctor Jekyll (condivisione) e signor Hyde (chiusura): la disciplina europea sui dati tra narrative e realtà

Il Regolamento EHDS si inserisce organicamente nella cornice del cosiddetto “diritto europeo dei dati”, trovando il suo fondamento nella European Data Strategy. Tale strategia mira a istituire un mercato unico dei dati che ne favorisca la libera circolazione tra i vari settori, a beneficio di imprese, ricerca e pubbliche amministrazioni. L’obiettivo principale consiste nella creazione di un ecosistema digitale trasparente ed equo, in cui il potenziamento del controllo dei cittadini sulle proprie informazioni personali funga da cardine per un quadro normativo affidabile.

In questo panorama complesso si intrecciano, come già ricordato, molteplici atti legislativi: il GDPR, la Direttiva Open Data, l’AI Act²³, il DGA e il DA²⁴. Tuttavia, questa stratificazione normativa rischia di generare un vero e proprio “effetto nebbia” regolatorio: l’eccessiva densità di regole può innalzare i costi transattivi e creare incertezza sull’applicazione delle norme nei diversi scenari. Il pericolo concreto è che, di fronte a rischi legali difficili da valutare, si assista a un disincentivo alla condivisione dei dati, rallentando l’innovazione che la stessa strategia intendeva promuovere.

Sussiste il rischio concreto di una frammentazione operativa derivante dalle modalità di attuazione nazionale della governance prevista da tali interventi. Sebbene l’obiettivo sia l’uniformità, la creazione di autorità di controllo e organismi di intermediazione a livello statale ricade nelle competenze dei singoli Paesi membri, con il rischio di generare divergenze applicative paradossali rispetto alle dichiarate finalità di armonizzazione.

23 Per approfondimenti sul suo contenuto si v., *ex plurimis*, C. Necati Pehlivan, N. Forgo, P. Valcke (a cura di), *The EU Artificial Intelligence (AI) Act*, Wolters Kluwer, 2025.

24 Inoltre, influiscono in modo diretto nello specifico contesto del trattamento di dati sanitari altre previsioni quali: la Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche), il Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano, il Regolamento europeo (UE) 2017/745 del Parlamento europeo e del Consiglio del 5 aprile 2017 sui dispositivi medici e la Direttiva 2011/24/UE sull’applicazione dei diritti dei pazienti relativi all’assistenza sanitaria transfrontaliera.

Sotto il profilo concettuale, nei documenti della Commissione Europea il paradigma dell’“apertura” e della “condivisione” appare progressivamente superato dal principio di “sovranità digitale”²⁵. Tale concetto, oggetto di un vivace dibattito dottrinale, delinea la facoltà degli Stati di disciplinare le attività digitali, specialmente quando queste incidono direttamente sui cittadini²⁶. Tuttavia, la regolamentazione di fenomeni intrinsecamente transnazionali e globali rimane una sfida complessa²⁷. Nel contesto UE, l’“Europe’s ability to act independently in the digital world” ha fornito nel 2020 una prima definizione²⁸. Da questo documento in poi l’approccio dell’Unione è stato sempre chiaramente politico più che giuridico e volto a promuovere una propria autonomia strategica in ambito digitale. In ciò provando a dare risposta alle minacce che le aziende ad alta tecnologia, di regola con sede in paesi extra-UE e che controllano il mercato degli strumenti e delle applicazioni digitali, hanno posto (le cosiddette “Big-Tech”)²⁹.

Emerge qui la classica divergenza tra narrazione e prassi applicativa. Se la narrativa unionale esalta l’efficacia dell’intervento regolatorio (livello declamatorio), la realtà operativa rivela una costellazione frammentata di regimi giuridici sovrapposti, tutti insistenti sul medesimo bene: il dato. In questo contesto viene così agevole citare, come metafora, la famosa opera «Lo strano caso del dottor Jekyll e del signor Hyde» di Robert Stevenson. Proprio come Jekyll descrive la sua trasformazione come

25 Cfr. G. Finocchiaro, *La sovranità digitale*, in *Diritto pubb.*, 2022, 3, 809-827; G. Resta, F. Simonetti, *La c.d. sovranità digitale e il progetto Gaia-X*, in *Contratto e imp.-Europa*, 2022, 3, 479-489; V. Zeno Zencovich, *Data Protection[ism]*, in *Media Laws*, 2022, 2, 1-9; L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Phil. & Tech.*, 2020, 369-378.

26 Cfr. S. Mangiameli, *La sovranità digitale*, in *Diritti fondamentali.it*, 2023, 3, 279-297; V. Bertola, *La sovranità digitale e il futuro di internet*, in *Riv. it. inf. dir.*, 2022, 1, 39-47.

27 Cfr. H. Roberts, *Digital sovereignty and artificial intelligence: a normative approach*, in *Ethics Inf Technol*, 2024, 26, (in Rete: <https://doi-org.ezp.biblio.unitn.it/10.1007/s10676-024-09810-5>).

28 Si v. T. Madiaga, *Digital sovereignty for Europe*, European Parliamentary Research Service, 2020, in Rete: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

29 Per maggiori approfondimenti si v. G. Bincoletto, R. Vardanian, G. Bellantuono, M. Ferrari, P. Guarda, *Digital and Data Sovereignty: the applicable legal frameworks and the case study of the IoT*, Trento: 2025, <https://zenodo.org/records/18015620>.

«qualcosa di indescrivibilmente nuovo e, per la sua stessa novità, incredibilmente dolce», anche la narrazione unionale si presenta con l'entusiasmo di una riforma epocale. Tuttavia, la realtà della "messa a terra" normativa rivela presto il suo volto più oscuro: un sistema che, lungi dal semplificare, si scopre – per usare le parole di Stevenson – «dieci volte più malvagio» a causa di una complessità che finisce per disincentivare proprio quegli obiettivi di condivisione che si prefiggeva di raggiungere. In tutto questo è possibile rintracciare un segnale di "speranza" nella disciplina sugli spazi di dati: perimetrare con precisione le criticità di uno specifico scenario facilita il compito di tecnici e giuristi impegnati nella costruzione di ecosistemi ed infrastrutture per il data sharing. Per ora accontentiamoci di questo, auspicando in un finale inedito rispetto all'opera di Stevenson.

In un contesto in cui i grandi colossi farmaceutici esercitano un controllo sempre più stretto sui dati clinici generati da ricerche finanziate con fondi pubblici, questo libro scava nelle tensioni tra privatizzazione della conoscenza e scienza aperta. Attraverso un'analisi rigorosa che spazia dalla filosofia politica al diritto comparato, passando per bioetica e prassi di governance, l'opera mette a fuoco i nodi strutturali che segnano la gestione e la condivisione dei dati clinici. Vengono esplorati i rischi insiti nella cultura della proprietà intellettuale e della pseudo-proprietà intellettuale (l'esclusiva sui dati clinici), nella datificazione pervasiva della medicina, nella mercificazione della salute e nelle derive della sorveglianza digitale. Con casi studio e proposte di politica del diritto, il volume mostra come la trasparenza, la riproducibilità della ricerca e la tutela dei soggetti coinvolti siano minacciate o favorite da regole, tecnologie e logiche di mercato. Una risorsa fondamentale per chiunque si interroghi su proprietà intellettuale, innovazione farmaceutica, diritto alla salute, protezione dei dati personali e scienza aperta. Il testo si rivolge sia a professionisti del settore sia a lettori attenti ai cambiamenti che attraversano il modo in cui ci curiamo oggi.

www.ledizioni.it