Il diritto alla protezione dei dati personali tra persona e mercato

Gabriele Carapezza Figlia[*], Michele Ciancimino[**]

Ricevuto 22 giugno 2026 – Accettato 13 luglio 2026

Sommario

Il contributo esamina il diritto alla protezione dei dati personali in prospettiva sistematico-assiologica. Dopo un inquadramento dell'evoluzione storica dalla riservatezza alla protezione dei dati personali, l'analisi ricostruisce l'impianto essenziale del REG UE 679/2016, con riguardo ai princípi, alla nozione di dato personale, alle categorie particolari, alle basi giuridiche del trattamento e ai diritti dell'interessato. La trattazione si sofferma, quindi, sulla dimensione economica del dato personale, sulla sua rilevanza nei rapporti contrattuali e sulla funzione assunta nei mercati digitali. Posta una lettura coordinata del più recente quadro regolatorio europeo – DSA, DGA, DMA, Data Act, AI Act, EHDS e proposta Digital Omnibus –, emerge una ricostruzione che, evitando tanto la patrimonializzazione piena quanto la riduzione del dato a mero oggetto di tutela negativa, valorizza dignità della persona e autodeterminazione informativa come parametri irriducibili anche nell'economia digitale.

Parole chiave: protezione dei dati personali, riservatezza, mercati digitali, GDPR, governance europea dei dati, intelligenza artificiale

[*] Università LUMSA. g.carapezzafiglia@lumsa.it.
[**] Università LUMSA. m.ciancimino@lumsa.it.

De Iustitia et Iure (ISSNe 3103-2761), 1/2026
DOI: 10.3280/ius2026oa23143

The right to personal data protection between the person and the market

Abstract

This article examines the right to personal data protection from a systematic and axiological perspective. After outlining the historical evolution from privacy to personal data protection, the analysis reconstructs the essential framework of Regulation (EU) 2016/679, with regard to its principles, the notion of personal data, special categories of data, lawful bases for processing and data subjects' rights. It then focuses on the economic dimension of personal data, its relevance within contractual relationships and the function it performs in digital markets. Against the background of a coordinated reading of the most recent European regulatory framework – the DSA, DGA, DMA, Data Act, AI Act, EHDS and the Digital Omnibus proposal – the article puts forward a reconstruction that avoids both full patrimonialisation and the reduction of personal data to a mere object of negative protection, while emphasising human dignity and informational self-determination as irreducible benchmarks also within the digital economy.

Keywords: personal data protection, privacy, digital markets, GDPR, European data governance, artificial intelligence

1. Considerazioni introduttive[1]

Tra le trasformazioni più significative che hanno interessato il diritto privato contemporaneo vi è certamente quella relativa alla protezione dei dati personali. Pochi ambiti dell'esperienza giuridica consentono infatti di cogliere con altrettanta evidenza le tensioni che attraversano la società contemporanea: il rapporto tra libertà e tecnologia, tra autonomia e controllo, tra diritti fondamentali ed efficienza economica, tra persona e mercato. La disciplina dei dati personali costituisce oggi uno dei principali luoghi nei quali tali tensioni si manifestano e richiedono di essere ricomposte entro un quadro coerente di princípi e regole.

La progressiva digitalizzazione delle relazioni sociali, economiche e istituzionali ha determinato una crescita esponenziale della produzione, raccolta, elaborazione e circolazione delle informazioni personali. Ogni attività svolta nell'ambiente digitale genera dati suscettibili di essere conservati, aggregati e utilizzati per una pluralità di finalità. In tale contesto, il dato personale non rappresenta più soltanto un elemento identificativo della persona

[1] Il contributo è frutto di una comune riflessione degli autori. Ai fini dell'attribuzione sono da ascrivere a Gabriele Carapezza Figlia il par. 1 e a Michele Ciancimino i parr. 2-7.

fisica, ma diviene un fattore strategico dell'economia contemporanea, una risorsa produttiva essenziale e uno degli elementi sui quali si fondano i modelli di business delle piattaforme digitali, i sistemi di profilazione algoritmica e le più recenti applicazioni dell'intelligenza artificiale.

L'emersione della cosiddetta "data economy" ha reso evidente come i dati personali siano divenuti una delle principali risorse dell'economia digitale. Le informazioni relative agli individui vengono raccolte e trattate per finalità di personalizzazione dei servizi, profilazione commerciale, pubblicità comportamentale, sviluppo di modelli predittivi e addestramento di sistemi intelligenti. La loro rilevanza economica è tale da avere indotto una parte della dottrina a interrogarsi sulla possibilità di ricostruire il fenomeno attraverso le categorie proprie della circolazione dei beni e del diritto patrimoniale.

Una simile prospettiva, tuttavia, coglie soltanto uno dei profili del fenomeno. Se è vero che i dati personali assumono una crescente rilevanza economica, è altrettanto vero che essi continuano a costituire una proiezione dell'identità della persona e della sua dignità. Il dato personale, definito da GDPR 4, n. 1 come qualsiasi informazione riguardante una persona fisica identificata o identificabile, presenta una natura intrinsecamente polifunzionale. Esso costituisce, al tempo stesso, elemento della personalità individuale, oggetto di attività economiche, fattore produttivo e risorsa strategica per l'innovazione tecnologica. Proprio questa pluralità di funzioni impedisce tanto di ricondurlo esclusivamente alla logica dei diritti della personalità quanto di assimilarlo integralmente a una qualsiasi "commodity" destinata allo scambio.

La polifunzionalità del dato personale ne evidenzia, altresì, l'inidoneità a essere ricondotto ai tradizionali modelli di appropriazione esclusiva propri dei diritti reali. Sebbene il dato conservi una dimensione non patrimoniale, in quanto elemento costitutivo dell'identità personale dell'interessato, esso assume contestualmente una rilevanza economica che lo rende suscettibile di utilizzazione da parte di terzi per finalità molteplici e socialmente rilevanti. Tale utilizzazione, tuttavia, non si traduce nell'acquisto di una situazione di appartenenza assimilabile a quella dominicale, ma si realizza attraverso attività di trattamento disciplinate da uno statuto normativo speciale, fondato sui princípi della protezione dei dati personali.

Ammettere che i dati personali abbiano un valore economico non implica, pertanto, l'adesione a una concezione proprietaria o rigidamente "market-oriented" della loro circolazione. Nell'ordinamento europeo il dato personale non costituisce, in quanto tale, un bene immateriale trasferibile secondo le categorie tradizionali della proprietà e della circolazione dei diritti. Ciò che forma oggetto di utilizzazione economica non è il dato in sé considerato, ma

l'insieme delle utilità che possono essere tratte dal suo trattamento, entro i limiti e secondo le modalità stabilite dalla disciplina della "data protection". Ne deriva un regime di circolazione speciale, che si distingue tanto dalla logica proprietaria quanto dai modelli ordinari dello scambio contrattuale.

In questa prospettiva, la negoziabilità dei dati personali non può essere esclusa facendo leva sulla loro natura non patrimoniale. Come da tempo evidenziato dalla dottrina civilistica, la negoziabilità di un bene non coincide con la sua patrimonialità, ma dipende dalla possibilità che l'atto di autonomia realizzi interessi meritevoli di tutela secondo l'ordinamento. La circostanza che il dato personale sia inerente alla sfera esistenziale della persona non ne impedisce, dunque, il coinvolgimento in operazioni negoziali; essa incide piuttosto sull'ampiezza e sulle modalità di esercizio dei poteri dispositivi, imponendo la predisposizione di limiti e garanzie coerenti con la natura del bene coinvolto.

Il problema centrale diviene allora quello di individuare un assetto regolatorio capace di conciliare l'inerenza del dato alla persona con la sua crescente rilevanza nei processi economici. La disciplina dei dati personali è chiamata a governare una realtà nella quale informazioni strettamente collegate all'identità individuale vengono continuamente raccolte, elaborate e valorizzate all'interno di mercati caratterizzati da forti asimmetrie informative e da rilevanti concentrazioni di potere economico e tecnologico.

Il diritto alla protezione dei dati personali si colloca pertanto all'intersezione tra differenti logiche ordinamentali. Esso rimane saldamente ancorato alla tutela della persona umana e all'esigenza di garantirne l'autodeterminazione informativa, ma al contempo è chiamato a confrontarsi con fenomeni di circolazione e valorizzazione economica delle informazioni che interessano il diritto dei contratti, il diritto dei consumatori, il diritto della concorrenza e la regolazione dei mercati digitali. La protezione dei dati personali costituisce così uno dei più significativi terreni nei quali il diritto contemporaneo è chiamato a misurarsi con il problema del rapporto tra persona e mercato.

Muovendo da tali premesse, il presente contributo intende ricostruire il diritto alla protezione dei dati personali in una prospettiva sistematico-assiologica, verificando come l'ordinamento europeo tenti di conciliare le esigenze di valorizzazione economica dei dati con la salvaguardia della dignità della persona e della sua libertà di autodeterminazione.

2. L'evoluzione storica: dalla privacy alla protezione dei dati

L'itinerario che ha condotto al riconoscimento del diritto alla protezione dei dati personali affonda le sue radici nella travagliata elaborazione giurisprudenziale del diritto alla riservatezza.

Nell'esperienza italiana, infatti, in assenza di un esplicito riconoscimento legislativo, la riservatezza si è imposta progressivamente, attraverso un dialogo tra la Corte di Cassazione e la Corte costituzionale, fra tradizione liberale e principio personalistico[2].

In un primo momento, si escluse che alla riservatezza possa riconoscersi autonoma tutela come situazione giuridica soggettiva (Cass. 22 ottobre 1956, n. 4487[3]). La posizione cominciò a essere messa in discussione nel 1963, allorché si ammise una tutela indiretta nell'alveo dei diritti assoluti della personalità, pur senza riconoscere autonomia alla riservatezza (Cass. 20 aprile 1963, n. 990[4]).

La svolta decisiva si registrò nel 1973, quando la Corte costituzionale riconobbe la riservatezza tra i diritti inviolabili dell'uomo ai sensi di Cost. 2 (Corte Cost. 12 aprile 1973, n. 38[5]). Pochi anni dopo, nel celebre "caso Soraya", la Cassazione attribuì alla riservatezza un duplice fondamento, esplicito (CEDU 8; 10) e implicito (Cost. 2; 3) (Cass. 27 maggio 1975, n. 2129[6]); a fine secolo l'orientamento è consolidato dal richiamo unitario al canone personalistico di Cost. 2 (Cass. 9 giugno 1998, n. 5658[7]).

In questa lunga gestazione, la riservatezza si presenta essenzialmente come situazione giuridica di carattere negativo: essa tutela l'individuo dall'intrusione altrui nella propria sfera privata, garantendo il "right to be let alone" teorizzato già nel noto saggio dottrinale statunitense[8]. Il bene protetto è il segreto della sfera personale; la tecnica di tutela è la rimozione dell'ingerenza esterna.

La protezione dei dati personali, per vero, muove da un'esigenza diversa e ulteriore: non soltanto evitare intrusioni, ma garantire all'individuo un potere di controllo continuo sulle informazioni che lo riguardano, una volta che esse siano state raccolte, organizzate ed elaborate da terzi. È in questa

[2] Per una ricostruzione recente dell'*iter* giurisprudenziale, cfr. Niger (2006) pp. 63 ss.; Gambini (2008); Visintini (2019).

[3] In *Giur. it.*, 1957, I, 1, 366 ss.

[4] In *Foro it.*, 1963, I, 877 ss.

[5] In *Giur. cost.*, 1973, 361 ss.

[6] In *Dir. aut.*, 1975, 351 ss.

[7] In *Dir. inf.*, 1999, 39 ss.

[8] Warren e Brandeis (1890) pp. 193 ss.

prospettiva che si colloca, anzitutto, l'autodeterminazione informativa, formula mutuata dalla giurisprudenza costituzionale tedesca, che esprime la pretesa del soggetto di essere signore delle informazioni che si riferiscono alla propria persona.

Sul piano del diritto europeo, il passaggio si è consolidato, in particolare, nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE), che, accanto alla protezione della vita privata (art. 7), riconosce in via autonoma il diritto alla protezione dei dati personali, qualificandolo come diritto fondamentale a struttura procedurale: i dati devono essere trattati lealmente, per finalità determinate, in base al consenso dell'interessato o ad altro fondamento legittimo previsto dalla legge; sono inoltre assicurati il diritto di accesso, di rettifica e il controllo da parte di un'autorità indipendente. TFUE 16 conferisce all'Unione la competenza ad adottare norme uniformi in materia, valorizzando la doppia funzionalità – protettiva e dinamica – di tale *corpus* normativo[9].

In questa traiettoria, la distinzione tra riservatezza e protezione dei dati personali non è meramente classificatoria: in termini schematici, la riservatezza presidia anzitutto il segreto della sfera privata; la protezione dei dati personali organizza, invece, il controllo partecipativo dell'interessato sul ciclo di trattamento delle informazioni che lo riguardano[10]. Si tratta, dunque, di un autonomo statuto della persona nell'ambiente informativo, non riducibile alla riservatezza ma con essa coordinato nella tutela dell'identità personale[11].

3. Il sistema del GDPR. I princípi

Il REG UE 679/2016 (GDPR) costituisce, nell'ordinamento dell'Unione e in quello interno, la fonte di riferimento del diritto alla protezione dei dati personali.

Tale regolamento ha profondamente innovato i fondamenti teorici e i meccanismi applicativi della protezione dei dati. Esso, infatti, per un verso individua una serie di regole di dettaglio utili al trattamento dei dati; per altro

[9] Cfr. Calzolaio (2017); de Hert (2015).

[10] V. Gambini (2008) p. 100, ove la protezione dei dati è qualificata come «dimensione dinamica» del diritto alla riservatezza.

[11] Per il passaggio dal segreto alla dignità, Perlingieri P. (2018) p. 484, ove si osserva che «il regolamento UE non è a tutela soltanto della riservatezza: esso disciplina più ampiamente la dignità della persona umana; la riservatezza ne è un aspetto, a volte relativo, e di certo non la esaurisce».

verso, offre una connotazione innovativa del diritto fondamentale qui in esame. Con riguardo a tale seconda declinazione, per vero, la protezione dei dati viene collocata dal GDPR fra le esigenze di funzione sociale che questa porta con sé[12] e le istanze mercantilistiche connesse alla libera circolazione dei dati[13].

La sua disciplina, oltre ad assicurare uniformità applicativa nello spazio europeo, definisce un sistema di princípi che operano quale parametro di legittimità di ogni trattamento[14]. GDPR 5 enumera tali princípi: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; responsabilizzazione ("accountability").

La portata sistematica di tali princípi è duplice[15].

Per un verso, essi orientano l'interpretazione delle norme di dettaglio del Regolamento, integrandone le formule generali (es.: adeguatezza, pertinenza, non eccedenza). Per altro verso, essi esprimono un'opzione di fondo del legislatore europeo: il passaggio da una concezione esclusivamente consensualistica della tutela a una concezione fondata sul controllo, nella consapevolezza che il consenso, da solo, non basta a garantire il rispetto della persona[16]. Da qui la centralità dei princípi di "accountability" (GDPR 24), di protezione fin dalla progettazione e per impostazione predefinita (GDPR 25) e di valutazione d'impatto sulla protezione dei dati (GDPR 35), che impongono al titolare obblighi conformativi sin dalla prima progettazione del trattamento.

In questa logica si colloca, in particolare, il principio di "accountability": il titolare non solo è tenuto a rispettare i princípi del Regolamento, ma deve altresì essere in grado di dimostrarne il rispetto. Esso si coordina con la prospettiva regolatoria fondata sul rischio: così, la legittimità del trattamento non può esaurirsi nell'adesione a procedure standardizzate *a priori*, ma richiede, essenzialmente, la proattività del titolare nella gestione dei potenziali rischi e la documentazione delle scelte adottate e della loro proporzionalità rispetto ai rischi per gli interessati[17].

[12] Rodotà (2006) p. 79; Ricci (2017) p. 604; Calabrese (2025) pp. 230 ss.

[13] Vettori (2024) p. 19.

[14] V. sul punto, anche per ulteriori riferimenti, Bravo (2023) pp. 38 ss.

[15] Per una ricostruzione del ruolo dei principi nel diritto della protezione dei dati, v. in particolare de Hert (2017) pp. 161 ss.

[16] Perlingieri P. (2018) pp. 481 ss., ove si osserva il passaggio da una concezione fondata esclusivamente sul consenso informato ad una focalizzata prevalentemente sul controllo.

[17] V. de Hert e Lazcoz (2022); Finocchiaro (2019) pp. 2779 ss.

4. Il sistema del GDPR. Profili applicativi

A monte dell'inquadramento assiologico si pone la nozione stessa di dato personale. GDPR 4, n. 1 definisce «dato personale» qualsiasi informazione riguardante una persona fisica identificata o identificabile, in termini di una definizione strutturalmente ampia, progressivamente estesa dalla giurisprudenza della Corte di giustizia[18].

A questa nozione si affianca quella, più selettiva, di «categorie particolari di dati personali» (GDPR 9): dati che rivelino origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona, dati sulla salute, sulla vita o sull'orientamento sessuale. La distinzione risponde a una logica di proporzionalità: quanto più il dato è idoneo a incidere sulla sfera più delicata della persona, tanto più stringente è la disciplina del trattamento. Sebbene l'art. 9 esordisca formalmente con un «divieto», la struttura del par. 2 – che individua le condizioni di ammissibilità del trattamento altrimenti vietato – risponde a una logica di tutela analoga a quella di GDPR 6, sia pure con presupposti più stringenti[19].

Al riguardo, giova chiarire che tali definizioni sono state, invero, interpretate in chiave funzionale, prediligendo una lettura *in concreto*, sulla base della effettiva possibilità di un dato di consentire l'identificazione, in ragione del contesto e delle modalità del trattamento, del soggetto interessato[20].

Il trattamento di dati personali, poi, è lecito soltanto se ed in quanto fondato su una delle basi giuridiche tassativamente elencate da GDPR 6, par. 1[21]: a) consenso dell'interessato; b) necessità per l'esecuzione di un contratto cui l'interessato è parte o di misure precontrattuali; c) necessità per l'adempimento di un obbligo legale; d) salvaguardia di interessi vitali; e) esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; f) perseguimento del legittimo interesse del titolare o di un terzo, salvo che prevalgano gli interessi e i diritti fondamentali dell'interessato. La tassatività dell'elenco è tradizionalmente riconosciuta dalla dottrina: il consenso non è la sola, né necessariamente la principale, base di liceità[22].

[18] Cfr. De Franceschi (2021) pp. 158 ss. V., poi, CGUE, 11 dicembre 2014, C-212/13, Ryneš (sulla videosorveglianza); CGUE, 19 ottobre 2016, C-582/14, Breyer (con riferimento all'indirizzo IP dinamico); CGUE, 20 dicembre 2017, C-434/16, Nowak (rispetto alle annotazioni dell'esaminatore durante un esame).

[19] Cfr. Ciancimino (2020) § 2.1.

[20] V. in particolare CGUE, Grande Sez., 4.10.2024, C-21/23, con nota di Bernes (2025).

[21] V. in particolare Orlando (2024b) pp. 831 ss., sulla nozione di liceità sostanziale del trattamento dei dati.

[22] Sulla tassatività delle basi di liceità di cui a GDPR 6, De Franceschi (2017) pp. 37 ss.

Particolare rilievo assume, in tale cornice, il consenso (GDPR 7), che deve essere libero, specifico, informato e inequivocabile[23]. Tali requisiti non sono meramente formali: la libertà postula l'assenza di condizionamenti e si scontra con la prassi delle architetture "pay-or-consent", nelle quali l'utente è chiamato a scegliere fra pagamento del servizio e cessione dei dati[24]; la specificità impone la frammentazione del consenso rispetto a ciascuna finalità del trattamento; l'informazione richiede una rappresentazione completa e comprensibile delle modalità e degli effetti del trattamento; l'inequivocabilità esclude consensi tacitamente desumibili da silenzio o inerzia. Il consenso, infine, è sempre revocabile, senza pregiudizio per la liceità del trattamento previamente eseguito.

Quando si tratti di categorie particolari di dati, le condizioni di liceità sono ulteriormente selezionate (GDPR 9, par. 2): consenso esplicito; adempimenti in materia di diritto del lavoro o di sicurezza sociale; salvaguardia di interessi vitali; trattamento da parte di organizzazioni non lucrative; dati manifestamente resi pubblici dall'interessato; accertamento o esercizio di un diritto in sede giudiziaria; motivi di interesse pubblico rilevante; finalità di medicina preventiva, diagnosi, cura, gestione di sistemi sanitari; interesse pubblico nel settore della sanità pubblica; archiviazione, ricerca scientifica o storica e statistica conformi all'art. 89, par. 1. Il legislatore europeo, dunque, costruisce un sistema di "eccezioni" tipizzate e garanzie rafforzate, che riconosce la rilevanza di interessi collettivi qualificati[25].

Sul piano dell'attribuzione di poteri all'interessato, il Capo III del GDPR riconosce un catalogo di diritti che ricostruiscono in capo al soggetto un controllo permanente sull'intero ciclo del trattamento: il diritto di accesso (art. 15), presupposto logico di tutti gli altri; il diritto di rettifica (art. 16) e di cancellazione (art. 17), che traducono il principio di esattezza e il c.d. diritto all'oblio; il diritto di limitazione (art. 18); il diritto alla portabilità dei dati (art. 20), che consente all'interessato di ricevere e trasferire i propri dati in formato strutturato, di uso comune e leggibile da dispositivo automatico; il diritto di opposizione (art. 21), che richiede al titolare di dimostrare motivi legittimi cogenti che prevalgono sull'interesse dell'interessato; il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento

[23] Sulle caratteristiche del consenso al trattamento, inteso come peculiare atto di autonomia privata, v. Orlando (2024a) pp. 336 ss.

[24] Sulla critica all'idoneità del consenso a presidiare la circolazione dei dati e, in particolare, sul modello "pay-or-consent", Thobani (2025) pp. 476 ss. V. altresì European Data Protection Board (EDPB) (2024).

[25] In tal senso, già Thobani (2019) pp. 144 ss. Cfr. Garante privacy, 27 febbraio 2025, n. 114 sui requisiti qualitativi del consenso al trattamento.

automatizzato, compresa la profilazione, idonea a produrre effetti giuridici o significativamente incidente (art. 22).

Tale catalogo non va letto in chiave enumerativa, ma sistematica: i diritti dell'interessato configurano una situazione giuridica permanente e dinamica, una sorta di *rei persecutio* informativa, quale persistenza di facoltà partecipative dell'interessato lungo le successive vicende del dato[26]. È a questo livello che si situa la peculiarità della disciplina europea: il dato personale, una volta uscito dalla sfera dell'interessato, non si emancipa definitivamente da tale sfera, ma porta con sé un fascio di facoltà partecipative che ne accompagna le successive vicende.

Cionondimeno, tale considerazione trova una potenziale criticità applicativa nelle dinamiche circolatorie secondarie dei dati personali, ossia quegli impieghi di dati personali diversi dalla finalità per cui i dati sono stati ceduti, ma ugualmente compatibili con l'uso primario, o comunque fondati nel trattamento principale[27].

5. Il dato personale come «moneta invisibile» dell'era digitale

L'impianto regolatorio del GDPR è chiamato oggi a operare in un contesto economico profondamente trasformato. Nei mercati digitali, il dato personale non è soltanto un'informazione riferibile a una persona fisica[28], ma costituisce, com'è noto, un fattore produttivo primario: alimenta i sistemi di profilazione algoritmica, sorregge i modelli commerciali fondati sulla raccolta pubblicitaria, abilita le strategie di personalizzazione dell'offerta e contribuisce al consolidamento del potere di mercato degli operatori dominanti[29].

Su questo terreno la dottrina si è divisa. Secondo un primo orientamento, il dato personale è riconducibile alla categoria del bene giuridico in senso ampio, idoneo ad assumere rilevanza patrimoniale e a fungere da contropartita di un servizio digitale. Una diversa impostazione esprime forte cautela rispetto alla patrimonializzazione del dato, ammonendo contro il rischio di

[26] La formula è usata in senso puramente descrittivo, per evocare la sequela di poteri che l'interessato conserva indipendentemente dalla circolazione del dato; cfr. Ciancimino (2022) pp. 62 ss.

[27] V. sul punto Perlingieri C. (2024) pp. 489 ss.; Bravo (2025); Iurilli (2024).

[28] Evidenzia le peculiarità applicative della ricostruzione dei dati in termini di attributi della personalità Martone (2026) pp. 191 ss.

[29] V., *amplius*, Savona (2026) pp. 88 ss.; Achille (2025) pp. 456 ss.; la Bella (2023) pp. 32 ss.; Ainis (2023) pp. 53 ss.; Ammannati (2021) pp. 112 ss.

una «monetizzazione della libertà» e contro la formazione di un «sottoproletariato del digitale»[30].

La ricostruzione che si predilige, invero, rifiuta tanto la patrimonializzazione piena quanto la riduzione del dato personale a mero oggetto di tutela negativa. Il dato personale, pur potendo considerarsi bene giuridico, rimane comunque una proiezione della personalità del soggetto, anche quando entra a comporre operazioni economiche, e non ne può essere disposto come di un bene patrimoniale puro, ma sempre nei limiti della disciplina di ordine pubblico contenuta nel GDPR e con il permanere del fascio di diritti dell'interessato[31]. Si tratta di un'osmosi, piuttosto che di una sostituzione: il dato resta indisponibile attributo della persona e, al contempo, può divenire oggetto di rapporti negoziali, secondo paradigmi nuovi rispetto al modello traslativo della compravendita[32].

In tal senso, se, per un verso, risulta necessario implementare una rilettura della protezione dei dati alla luce del diritto delle obbligazioni e dei contratti[33], sì da favorirne una migliore compatibilità con le peculiari manifestazioni dell'economia digitale, per altro verso deve ugualmente garantirsi un margine di controllo e di tutela sulle dinamiche relative a tale situazione giuridica, in ragione dei riflessi personalistici ad essa connessi.

In questa direzione si è mosso il diritto europeo dei contratti, in particolare con la DIR UE 770/2019 (sui contenuti e servizi digitali). Il legislatore europeo, sollecitato dalla posizione critica del Garante europeo della protezione dei dati[34], ha evitato di qualificare espressamente i dati personali come «controprestazione», ma ha riconosciuto la rilevanza giuridica dello scambio fra fornitura del servizio e cessione del dato; DIR UE 770/2019, cons. n. 24 chiarisce che i dati personali non possono essere considerati una merce, pur riconoscendo la rilevanza del rapporto per l'ambito di applicazione della direttiva[35].

La giurisprudenza italiana ha contribuito a una certa pacificazione fra i

[30] Stanzione (2023) p. 162. Cfr. sul dibattito Matta (2025) pp. 20 ss.; Morace Pinelli (2023) pp. 9 ss.; Ricciuto (2019).

[31] Cfr. Perlingieri P. (2003).

[32] Ciancimino (2022) p. 63.

[33] De Franceschi (2017) spec. pp. 111 ss. V. anche il considerando n. 24, DIR UE 770/2019, il quale, da un lato, riconosce che i dati personali non possono essere considerati una merce e, dall'altro, che i consumatori hanno diritto a rimedi contrattuali nei modelli commerciali basati sul trattamento di dati.

[34] European Data Protection Supervisor (EDPS) (2017). Cfr. sul tema Orlando (2023) pp. 226 ss.

[35] Per il dibattito sulla qualificazione di tale rapporto v. Morace Pinelli (2023) pp. 21 ss.; Purpura (2022); Irti (2021) pp. 119 ss.; Camardi (2019).

due piani. Particolarmente significativa è la vicenda Facebook/AGCM, sviluppatasi tra il provvedimento dell'Autorità n. 27432/2018 e le successive pronunce di TAR Lazio e di Consiglio di Stato (TAR Lazio Sez. I 10 gennaio 2020, n. 261; CdS Sez. VI 29 marzo 2021, n. 2631)[36]. In quella sede è stato riconosciuto il «valore economico del patrimonio informativo» degli utenti e qualificata come pratica commerciale scorretta l'omessa rappresentazione di tale dimensione economica al momento dell'adesione al servizio.

Si è così formata, anche grazie all'"enforcement" consumeristico, una tutela multilivello: il GDPR garantisce la liceità del trattamento e la persistenza dei diritti dell'interessato; la disciplina consumeristica intercetta l'asimmetria informativa nell'adesione al servizio; il diritto della concorrenza interviene quando lo sfruttamento del dato è strumento di posizioni dominanti[37]. Tale convergenza genera una stratificazione delle tutele, coerente con la natura plurale del fenomeno: il dato è, a un tempo, attributo della persona, oggetto di scambio contrattuale e fattore competitivo.

La qualificazione del dato come "moneta invisibile" dell'era digitale è dunque evocativa, ma non esauriente: il dato non è moneta in senso tecnico, perché non possiede né la fungibilità né la disponibilità che caratterizzano i mezzi di pagamento; nondimeno, esso costituisce risorsa primaria nei mercati a due (o più) versanti tipici dell'ecosistema digitale, ove la fruizione apparentemente "gratuita" di un servizio è, in realtà, sostenuta da una valorizzazione economica del dato. Il "consenso" dell'interessato, in tali contesti, non è gratuito: la gratuità è soltanto apparente, perché attribuisce all'operatore il potere di gestione dei dati personali e, attraverso il loro trattamento, di trarne profitto[38].

L'osservazione conduce a una conseguenza sistematica rilevante. Il diritto alla protezione dei dati personali, lungi dall'essere disciplina meramente di garanzia individuale, può concorrere alla conformazione dell'ordine pubblico economico dei mercati digitali, poiché incide sulle condizioni di concorrenza, sull'asimmetria informativa e sulla contendibilità dei mercati "data-driven"; così, la tecnica regolatoria, conformando i rapporti di mercato, tende a rendere quell'ecosistema economico sempre più "sostenibile"

[36] Per la ricostruzione del caso v. Morace Pinelli (2023) pp. 17 ss. Il Consiglio di Stato ha precisato che «il corrispettivo per l'accesso al servizio offerto dalla società di *social network* non è rappresentato dalla cessione dei propri dati personali da parte degli utenti – secondo il modello traslativo della compravendita –, ma dalla messa a disposizione dei dati stessi».

[37] Cfr. Purpura (2022) pp. 911 ss.

[38] Così Perlingieri P. (2018) p. 484: «il consenso concesso non è gratuito: la gratuità è soltanto apparente».

per la persona dell'utente[39]. Da qui l'esigenza di un approccio sistematico, capace di integrare la disciplina della "data protection" con quella consumeristica e antitrust[40].

6. La governance europea tra protezione e valorizzazione: DSA, DGA, DMA, Data Act, AI Act nel sistema europeo dei dati

L'inadeguatezza di un approccio compartimentale ha indotto l'Unione europea a elaborare, a partire dal 2020, una strategia organica per la governance dei dati: l'emersione della necessità di regolare i poteri privati nei mercati digitali[41] ha messo in luce, da un lato, la rilevanza della protezione dei dati rispetto a tale esigenza, stante la centralità delle informazioni in un'economia "data-driven"[42]; dall'altro, l'impossibilità di delegare ogni profilo regolatorio al solo GDPR[43].

La Strategia europea per i dati[44] si articola su tre pilastri: la costruzione di un mercato interno dei dati; la promozione di spazi comuni di dati in settori strategici (sanità, mobilità, ambiente, finanza, agricoltura, manifattura); l'edificazione di un'infrastruttura tecnico-giuridica europea che ne consenta la circolazione e il riuso. Si è così formata, in pochi anni, una vera e propria trama regolatoria, definita da una parte della dottrina come il *corpus iuris digitalis* dell'Unione[45], composta principalmente, per quanto qui rileva, oltre che dal GDPR, dal Digital Services Act (REG UE 2065/2022), dal Digital Markets Act (REG UE 1925/2022), dal Data Governance Act (REG UE 868/2022), dal Data Act (REG UE 2854/2023), dall'AI Act (REG UE 1689/2024) e dal Regolamento sullo Spazio europeo dei dati sanitari (REG UE 327/2025).

Giova preliminarmente chiarire che i nuovi e più recenti interventi non sostituiscono il GDPR, ma vi si affiancano. Il GDPR conserva il ruolo di *lex*

[39] V. sul punto Corrias (2022) pp. 972 ss.

[40] Sulla «funzione sociale» richiamata da GDPR cons. n. 4 e sull'esigenza di una tutela multilivello v. Morace Pinelli (2023) pp. 6 ss.

[41] Sul tema, v., *ex multis*, Luchena (2025) pp. 253 ss.; Rametta (2025) pp. 925 ss.; Sciarrone Alibrandi (2021); Antonucci (2021) pp. 96 ss.

[42] Sulla centralità del trattamento dei dati nelle nuove tecnologie digitali e sulle correlate istanze regolatorie, v. Ricciuto (2025), p. 4.

[43] Cfr. de Hert e Cocito (2024).

[44] Comm. UE, 19 febbraio 2020, *Una strategia europea per i dati*, COM(2020) 66 final, in *ec.europa.eu*.

[45] Tosi (2025) p. 682.

generalis di tutela della persona[46]; i nuovi atti si occupano di profili strutturali del mercato (DSA, DMA), di condivisione e accesso ai dati (DGA, Data Act), di gestione del rischio nei sistemi di intelligenza artificiale (AI Act) e di organizzazione settoriale dei flussi di dati (EHDS). Si tratta, dunque, di una stratificazione regolatoria nella quale la tutela dei dati personali si integra con discipline che valorizzano specifiche declinazioni della libera circolazione del dato, anche in vista di obiettivi di interesse pubblico e di sviluppo economico[47].

Il Data Governance Act introduce un quadro normativo per il riutilizzo di dati detenuti da enti pubblici, per le organizzazioni di intermediazione dei dati (c.d. data intermediaries) e per l'altruismo dei dati. Esso ambisce a costruire un'infrastruttura fiduciaria della condivisione, riducendo l'asimmetria informativa e introducendo nuovi soggetti – fra cui le cooperative di dati (DGA, 2, par. 1, n. 15) – capaci di esercitare un'azione collettiva a tutela della posizione degli interessati[48]. Per i dati personali, gli intermediari devono assicurare un'effettiva separazione fra le proprie attività e quelle di altri servizi, evitando conflitti di interesse e garantendo la centralità della scelta dell'interessato.

Il Data Act, complementare al DGA, persegue la finalità di garantire un accesso equo ai dati generati dall'uso di prodotti connessi e di servizi correlati ("Internet of Things"), affiancando alla portabilità *ex* GDPR 20 un autonomo regime di accesso, condivisione e riutilizzo dei dati generati da prodotti connessi e servizi correlati. La disciplina, pertanto, interviene per riequilibrare le asimmetrie informative e contrattuali nei prodotti connessi, prevenire fenomeni di c.d. "lock-in" tecnologico e rendere accessibili e riutilizzabili i dati generati da dispositivi e servizi digitali[49].

Sul versante dei mercati digitali, il Digital Services Act introduce regole asimmetriche per gli intermediari della società dell'informazione, in particolare per le piattaforme e i motori di ricerca molto grandi (VLOP e VLOSE), imponendo obblighi di trasparenza, valutazione e mitigazione dei rischi sistemici (artt. 34-35), divieto di interfacce manipolative (art. 25), trasparenza dei sistemi di raccomandazione (artt. 27 e 38) e tutela particolare dei minori

[46] Anche e soprattutto in forza della sua regolazione eminentemente "per principi", che consente al GDPR di mantenere una certa attualità – "future-proof", nell'approccio del legislatore europeo – anche a distanza di dieci anni dalla sua emanazione.

[47] Cfr. Finocchiaro (2025) pp. 61 ss.; Tosi (2025) pp. 684 ss.; Cavalcanti e Nava (2024) pp. 232 ss.

[48] Sulle cooperative di dati e sulla governance duale v. Bravo (2026) pp. 115 ss.

[49] Per un approfondimento v. Zikesch, Sörup e Adrian (2026) pp. 6 ss.; Orlando (2025) pp. 50 ss.

(art. 28). Il Digital Markets Act, da parte sua, individua doveri *ex ante* a carico dei c.d. "gatekeeper", fra cui il divieto, in determinate condizioni, di combinare dati personali raccolti dai diversi servizi senza un consenso validamente prestato dall'utente ove necessario (DMA, 5, par. 2). Tali norme intercettano direttamente la dimensione concorrenziale del dato personale, completando la cornice di tutela già assicurata dal GDPR[50].

L'AI Act, da ultimo, regola il ciclo di vita dei sistemi di intelligenza artificiale secondo un approccio fondato sul rischio (rischio inaccettabile, alto rischio, rischio limitato, rischio minimo)[51]. Esso non sostituisce il GDPR, ma si coordina con esso[52], confermando che le tutele sostanziali in materia di dati personali permangono integre[53], quantomeno sul piano teoretico. Resta ferma la previsione di specifiche ipotesi settoriali – come AI Act, 10 – nelle quali il trattamento di categorie particolari di dati è ammesso entro condizioni rigorose.

In àmbito settoriale, il Regolamento sullo Spazio europeo dei dati sanitari (EHDS, REG UE 327/2025) realizza il primo «spazio comune dei dati» a livello di Unione. Esso disciplina l'uso primario dei dati sanitari (per finalità di cura) e l'uso secondario (ricerca, formazione, statistica, sanità pubblica), introduce diritti rafforzati dell'interessato (es.: accesso immediato e gratuito in formato europeo, EHDS, 3) e, soprattutto, segna, nel settore sanitario, uno spostamento del baricentro dal consenso individuale verso basi e procedure di interesse pubblico, controbilanciate da garanzie organizzative, controlli istituzionali e, per l'uso secondario, dal diritto di "opt-out"[54].

Il descritto assetto, invero, è attualmente soggetto a un rilevante intervento di revisione: la proposta "Digital Omnibus", presentata dalla Commissione europea il 19 novembre 2025, persegue una semplificazione del quadro regolatorio digitale, intervenendo trasversalmente, fra l'altro, sul GDPR, sull'AI Act, sul Data Act[55].

Per quanto qui interessa, due modifiche meritano particolare attenzione. La prima riguarda la nozione stessa di dato personale. La Commissione[56]

[50] Ainis (2023) pp. 59 ss.

[51] Per la cornice assiologica entro cui inscrivere il rapporto fra intelligenza artificiale e diritto civile v. Perlingieri P. (2025) pp. 137 ss.

[52] AI Act, conss. 10; 68.

[53] Tosi (2025) pp. 685 ss. e p. 711.

[54] Sul punto Faillace (2025) pp. 187 ss.; Pellegrini e Foà (2025) pp. 189 ss.

[55] Comm. UE, 19 novembre 2025, *Proposta di Regolamento del Parlamento europeo e del Consiglio (…)*, COM(2025) 837 final; Comm. UE, 19 novembre 2025, *Proposta di Regolamento (…)* (*Digital Omnibus on AI*), COM(2025) 836 final; *Commission Staff Working Document* SWD(2025) 836 final, 19 novembre 2025, sez. 1.1 ss. e cap. 3.

[56] Sulla scorta di CGUE, 4 settembre 2025, C-413/23 P, EDPS c. SRB.

propone di chiarire che un'informazione non costituisce dato personale per un soggetto che non disponga di mezzi ragionevolmente disponibili per identificare la persona cui essa si riferisce e introduce un meccanismo ("implementing acts") per la determinazione di quando dati pseudonimizzati possano considerarsi non personali per determinate entità. Si tratta di una potenziale «relativizzazione» della nozione di dato personale che intende coniugare la tutela della persona con lo sviluppo del mercato, ma che è stata oggetto di marcate riserve[57].

La seconda modifica concerne il rapporto fra GDPR e sviluppo di sistemi di intelligenza artificiale. La proposta intende introdurre un nuovo GDPR 88-*quater*, che riconosce il «legittimo interesse» (GDPR 6, par. 1, lett. f) come base giuridica per il trattamento di dati personali finalizzato allo sviluppo e al funzionamento di sistemi e modelli di intelligenza artificiale, salvo che altre disposizioni richiedano espressamente il consenso. Parallelamente, si propone una ulteriore deroga al divieto di trattamento di categorie particolari di dati *ex* GDPR 9, applicabile quando dati particolari siano "residualmente" presenti nei "dataset" di riferimento[58].

Le proposte, ancora *in itinere*, hanno suscitato un dibattito intenso, nel quale le esigenze di semplificazione e competitività sono poste a confronto con il rischio di attenuazione delle garanzie individuali[59].

Il "Digital Omnibus" sembra mostrare, ad ogni modo, l'esistenza di una tensione interna al sistema europeo dei dati. Da un lato, la cornice del GDPR esprime un'opzione personalistica: la centralità della persona, l'autodeterminazione informativa, la responsabilizzazione del titolare, l'attribuzione di un fascio di diritti partecipativi all'interessato. Dall'altro, le proposte di semplificazione e il movimento verso la valorizzazione economica del dato (DGA, Data Act, EHDS, oggi "Digital Omnibus") rispondono a un'esigenza di costruzione del mercato unico dei dati e di promozione della competitività europea, anche nei confronti dei grandi operatori extra-UE. Il punto di equilibrio fra le due esigenze non è dato una volta per tutte, ma è oggetto di un continuo aggiustamento, nel quale l'interprete è, invero, chiamato a un ruolo decisivo[60].

[57] Sul punto, cfr. Scognamiglio (2026) pp. 75 ss. V., poi, European Data Protection Board (EDPB) e European Data Protection Supervisor (EDPS) (2026b); per il Digital Omnibus on AI v. European Data Protection Board (EDPB) e European Data Protection Supervisor (EDPS) (2026a).

[58] Cfr. Italia (2026) pp. 285 ss.

[59] Cfr. sulle potenziali criticità del Digital Omnibus, Aloisi (2026); Italia (2026); Scognamiglio (2026).

[60] Sulle difficoltà di armonizzazione fra le varie fonti del sistema dei dati, cfr. Tommasi (2023).

7. Considerazioni conclusive. Mercati digitali e nuove frontiere

L'analisi condotta consente di trarre alcune conclusioni, necessariamente parziali in ragione della complessità del tema e della rapidità delle trasformazioni in atto.

Sul piano teorico, il diritto alla protezione dei dati personali si conferma situazione giuridica complessa, non riducibile alla riservatezza intesa quale *ius excludendi alios* né alla mera disponibilità economica del dato. Esso ha la propria radice nella dignità della persona e nel principio personalistico (Cost. 2; Carta UE 8) e si esprime nell'autodeterminazione informativa quale fascio di facoltà partecipative che accompagnano l'intero ciclo del trattamento. Il passaggio dal segreto al controllo – e dalla quiescenza dell'astensione di terzi all'attività permanente del soggetto sui propri dati – costituisce la cifra distintiva della disciplina contemporanea.

Sul piano sistematico, il sistema delle basi giuridiche (GDPR 6) e il catalogo dei diritti dell'interessato (GDPR 15-22) si rivelano le due facce di una medesima medaglia: l'ingresso del dato nel circuito del trattamento è subordinato a presupposti rigorosi di liceità, e la persistenza del controllo del soggetto è assicurata da una sequenza di poteri che mantengono in capo all'interessato la qualità di centro di imputazione delle informazioni che lo riguardano. Il consenso, in tale quadro, non è la sola né necessariamente la principale base giuridica: esso si inscrive in un sistema plurale, nel quale il legislatore riconosce la legittimità di trattamenti fondati su interessi pubblici o privati qualificati, purché contemperati con i diritti dell'interessato.

Sul piano evolutivo, i mercati digitali e le tecnologie di intelligenza artificiale rendono urgente un ripensamento degli strumenti di tutela. Il consenso, da solo, non è più in grado di assicurare la pienezza dell'autodeterminazione in contesti caratterizzati da profonde asimmetrie informative, da tecniche di progettazione persuasive e da modelli commerciali fondati sulla cattura dell'attenzione. La regolazione europea ha risposto con nuovi atti normativi (DGA, Data Act, DSA, DMA, AI Act, EHDS), che valorizzano la dimensione economica e infrastrutturale del dato pur senza rinunciare alla cornice di tutela del GDPR. Tale panorama, tuttavia, mostra oggi tensioni interne che la proposta "Digital Omnibus" pare rendere ancor più evidenti.

L'ordinamento europeo si trova, in questo momento, di fronte a una scelta delicata: se orientare il sistema della governance dei dati verso la valorizzazione economica tout-court, accettando il rischio di un progressivo svuotamento delle garanzie individuali; ovvero se mantenere la centralità della

persona, accettando la complessità di una regolazione plurale ma coerente con l'impostazione personalistica[61].

Il tratto distintivo del modello europeo – per quanto ancora imperfetto e attraversato da tensioni non risolte – sembra allora consistere nel continuo tentativo di coniugare innovazione, circolazione e sfruttamento dei dati con la preservazione della centralità della persona, entro un quadro regolatorio che assume la dignità del soggetto e l'autodeterminazione informativa come parametri irriducibili. Il dato personale, anche quando assume valore patrimoniale, non cessa di essere proiezione della personalità. Riconoscere questa specificità, evitando tanto le derive "proprietarie" quanto le rigidità che soffocano l'innovazione, costituisce il compito di una attività ermeneutica che voglia confrontarsi con la trasformazione digitale senza rinunciare al proprio radicamento assiologico.

Riferimenti bibliografici

Achille D. (2025). *Consenso e accordo nel mercato delle piattaforme digitali*. In: *Persona e Mercato*, 2: 453-467.

Ainis M. (2023). *Circolazione dei dati personali e disciplina del mercato*. In: Morace Pinelli A., a cura di (2023). *La circolazione dei dati personali: persona, contratto e mercato*. Pisa.

Aloisi A. (2026). *"Undo something, whatever it takes". The impact of the EU Digital Omnibus on workers*. In corso di pubblicazione in Rainone S. and Zwysen W., editor, *Regulating AI through collective bargaining – key issues*. Testo disponibile al sito: https://ssrn.com/abstract=6438041. DOI: 10.2139/ssrn.6438041.

Ammannati L. (2021). *La circolazione dei dati: dal consumo alla produzione*. In: Lener R., Luchena G. e Robustella C., a cura di, *Mercati regolati e nuove filiere di valore*. Torino.

Antonucci A. (2021). *Il mercato dei dati: dall'ecosistema separato alla regola trasversale*. In: Lener R., Luchena G., Robustella C., a cura di, *Mercati regolati e nuove filiere di valore*. Torino.

Bernes A. (2025). *La nozione di «dati relativi alla salute» al vaglio della Corte di Giustizia: quali conseguenze per il commercio elettronico e la concorrenza?* In: *Nuova giur. civ. comm.*, 3: 588-601.

Bravo F. (2023). *I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, nel solco*

[61] Cfr. sul punto il c.d. Rapporto Draghi – Draghi (2025a) pp. 23 ss.; Draghi (2025b) pp. 79 ss. –, per il quale l'approccio regolatorio europeo rischia di soffocare lo sviluppo tecnologico, frenando l'innovazione soprattutto per le piccole e medie imprese.

delle rules of construction. In: Bravo F., a cura di, *Dati personali. Protezione, libera circolazione e governance. 1. Principi*. Vol. 1. Pisa.
Bravo F. (2025). *L'intermediazione dei dati e la sua evoluzione dal settore privato a quello pubblico*. In: *Riv. it. dir. inf.*, 7(2): 259-294. DOI: 10.32091/RIID0243.
Bravo F. (2026). *Le cooperative di dati tra innovazione e tutela rafforzata degli interessati*. In: De Belvis E., a cura di, *Architetture giuridiche per la transizione digitale. Dialoghi interdisciplinari per governare la tecnologia*. Napoli.
Calabrese G. (2025). *La protezione dei dati personali tra individuo e società*. Milano.
Calzolaio S. (2017). *Protezione dei dati personali*. In: *Digesto, Disc. pubbl., Agg.*: 594-635.
Camardi C. (2019). *Prime osservazioni sulla direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*. In: *Giust. civ.*, 3: 499-523.
Cavalcanti S. e Nava G. (2024). *I rapporti tra AI Act e gli altri regolamenti in materia di dati*. In: Cassano G. e Tripodi E.M., a cura di, *Il Regolamento Europeo sull'Intelligenza Artificiale. Commento al Reg. UE n. 1689/2024*. Rimini.
Ciancimino M. (2020). *Protezione e controllo dei dati in àmbito sanitario e Intelligenza Artificiale. I dati relativi alla salute tra novità normative e innovazioni tecnologiche*. Napoli.
Ciancimino M. (2022). *Circolazione secondaria di dati sanitari. Nuovi paradigmi contrattuali e istanze personalistiche*. In: *Diritto di Famiglia e delle Persone*, 51(1): 37-69.
Corrias P. (2022). *Il mercato come risorsa della persona vulnerabile*. In: *Riv. dir. civ.*, 68(5): 968-990.
De Franceschi A. (2017). *La circolazione dei dati personali tra privacy e contratto*. Napoli.
De Franceschi A. (2021). *Art. 4 GDPR*. In: D'Orazio R., Finocchiaro G., Pollicino O. e Resta G., a cura di, *Codice della privacy e data protection*. Milano.
de Hert P. (2015). *The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents?*. In: *Utrecht J. of International and European L.*, 31(80): 1-4. DOI: 10.5334/ujiel.cz.
de Hert P. (2017). *Data protection as bundles of principles, general rights, concrete subjective rights and rules: Piercing the veil of stability surrounding the principles of data protection*. In: *European Data Protection Law Review*, 3(2): 160-179. DOI: 10.21552/edpl/2017/2/6.
de Hert P. e Cocito C. (2024). *The added value of data protection within the framework of digital constitutionalism in Europe*. In: De Gregorio G., O. Pollicino O. and Valcke P. (editor), *The Oxford handbook of digital constitutionalism*. Oxford. DOI: 10.1093/oxfordhb/9780198877820.013.34.
de Hert P. e Lazcoz G. (2022). *When GDPR-principles blind each other: Accountability, not transparency, at the heart of algorithmic governance*. In: *European Data Protection Law Review*, 8(1): 31-40. DOI: 10.21552/edpl/2022/1/7.
Draghi M. (2025a). *The future of European competitiveness. Part A. A*

competitiveness strategy for Europe. Lussemburgo. DOI: 10.2872/9356120 (pdf); DOI: 10.2872/1823372 (stampa).
Draghi M. (2025b). *The future of European competitiveness. Part B. In-depth analysis and recommendations*. Lussemburgo.
European Data Protection Board (EDPB) (2024). *Parere 8/2024 sul consenso valido nel contesto dei modelli "consenso o pagamento" attuati dalle piattaforme online di grandi dimensioni*. Testo reperibile in *edpb.europa.eu*.
European Data Protection Board (EDPB) e European Data Protection Supervisor (EDPS) (2026a). *Joint Opinion 1/2026*. Testo reperibile in *edpb.europa.eu*.
European Data Protection Board (EDPB) e European Data Protection Supervisor (EDPS) (2026b). *Joint Opinion 2/2026*. Testo disponibile al sito: *edpb.europa.eu*.
European Data Protection Supervisor (EDPS) (2017). *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*. Testo reperibile in *edps.europa.eu*.
Faillace S. (2025). *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS*. Milano.
Finocchiaro G. (2019). *Il principio di accountability*. In: *Giur. it.*: 2778-2783.
Finocchiaro G. (2025). *Diritto dell'intelligenza artificiale*. Bologna.
Gambini M. (2008). *Dati personali e internet*. Napoli.
Irti C. (2021). *Consenso "negoziato" e circolazione dei dati personali*. Torino.
Italia E. (2026). *L'impatto dell'intelligenza artificiale sull'attività giurisdizionale*. In: De Belvis E., a cura di, *Architetture giuridiche per la transizione digitale. Dialoghi interdisciplinari per governare la tecnologia*. Napoli.
Iurilli C. (2024). *La tutela del dato personale alla prova del Data Governance Act. Data sharing, reclamo e tutela giurisdizionale effettiva*. In: *Judicium*, 5 marzo 2024: 1-13.
la Bella A. (2023). *Sfide, opportunità e minacce nell'economia* data-driven. In: Morace Pinelli A., a cura di, *La circolazione dei dati personali: persona, contratto e mercato*. Pisa.
Luchena G. (2025). *Nuove tecnologie e regolazione del mercato*. In: *Assicurazioni*, 2: 246-267.
Martone I. (2026). *I dati personali quali attributi della personalità*. In: De Belvis E., a cura di, *Architetture giuridiche per la transizione digitale. Dialoghi interdisciplinari per governare la tecnologia*. Napoli.
Matta N. (2025). *Circolazione dei dati relativi alla persona e rapporti giuridici*. Napoli.
Morace Pinelli A., a cura di (2023). *La circolazione dei dati personali: persona, contratto e mercato*. Pisa.
Niger S. (2006). *Le nuove dimensioni della privacy*. Padova.
Orlando S. (2023). *Il coordinamento tra la direttiva 2019/770 e il GDPR. L'interessato-consumatore*. In: *Persona e Mercato*, 2: 222-241.
Orlando S. (2024a). *Consenso al trattamento e liceità*. In: *Persona e Mercato*, 2: 333-364.
Orlando S. (2024b). *Sulla necessità di un controllo di liceità sostanziale per tutte le basi del trattamento dei dati personali*. In: *Persona e Mercato*, 3: 815-845.

Orlando S. (2025). *La definizione di "dati" contenuta nel Data Act e la sua rilevanza nelle discipline dei vari capi del Regolamento*. In: Morace Pinelli A., a cura di, *Data Act. Introduzione interdisciplinare e commentario al Regolamento (UE) 2023/2854*. Pisa.
Pellegrini M. e Foà D. (2025). *Governance dei dati sanitari e intelligenza artificiale nella sanità pubblica*. In: Capriglione F., a cura di, *Sanità Finanza Etica*. Torino.
Perlingieri C. (2024). *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*. In: *Tecn. dir.*, 2: 485-509.
Perlingieri C. (2025). *Intelligenza artificiale tra principi e regole*. In: *AI Law*, 1: 35-47.
Perlingieri P. (1972). *La personalità umana nell'ordinamento giuridico*. Napoli (rist. 1982).
Perlingieri P. (2003). *L'informazione come bene giuridico*. In: Perlingieri P., *Il diritto dei contratti fra persona e mercato*. Napoli.
Perlingieri P. (2018). *Privacy e protezione dei dati personali*. In: *Foro nap.*, 2: 481-484.
Perlingieri P. (2020). *Sul trattamento algoritmico dei dati*. In: *Tecn. dir.*, 1: 181-194.
Perlingieri P. (2025). *Diritto civile e Intelligenza Artificiale*. In: *Tecn. dir.*, 1: 135-151.
Purpura A. (2022). *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei big data*. In: *Jus Civile*, 4: 891-916.
Rametta R. (2025). *La* governance *del mercato digitale europeo*. In: *Persona e mercato*, 3: 921-931.
Ricci A. (2017). *Sulla «funzione sociale» del diritto alla protezione dei dati personali*. In: *Contr. impr.*, 2: 586-612.
Ricciuto V. (2019). *La patrimonializzazione dei dati personali*. In: V. Cuffaro, R. D'Orazio e V. Ricciuto, a cura di, *I dati personali nel diritto europeo*. Torino.
Ricciuto V. (2022). *L'equivoco della privacy. Persona* vs *dato personale*, Napoli.
Ricciuto V. (2023). *Il consenso negoziale nella circolazione dei dati personali*. In: Morace Pinelli A., a cura di, *La circolazione dei dati personali: persona, contratto e mercato*. Pisa.
Ricciuto V. (2025). *Intelligenza artificiale e protezione dei dati*. In: *EJPLT. Special Issue 2025*, 1: 2-14. DOI: 10.57230/ejplt25sibvr.
Rodotà S. (2006). *La vita e le regole*. Milano.
Savona M. (2026). *Valore dei dati e* governance *dei dati*. In: De Belvis E., a cura di, *Architetture giuridiche per la transizione digitale. Dialoghi interdisciplinari per governare la tecnologia*. Napoli.
Sciarrone Alibrandi A. (2021). *Innovazione tecnologica e regolazione dei mercati*. In: Lener R., Luchena G. e Robustella C., a cura di, *Mercati regolati e nuove filiere di valore*, Torino.
Scognamiglio C. (2026). *Dati personali, pseudonimizzazione e anonimizzazione: una breve rassegna circa alcune recenti novità*. In: De Belvis E., a cura di, *Architetture giuridiche per la transizione digitale. Dialoghi interdisciplinari per governare la tecnologia*. Napoli.

Stanzione P. (2023). *Conclusioni*. In: Morace Pinelli A., a cura di, *La circolazione dei dati personali: persona, contratto e mercato*. Pisa.
Thobani S. (2019). *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*. In: *Medialaws*, 3: 131-147.
Thobani S. (2025). *Il consenso nella regolazione della circolazione dei dati*. In: *Persona e mercato*, 2: 469-486.
Tommasi S. (2023). *Digital Services Act e Artificial Intelligence Act: tentativi di futuro da armonizzare*. In: *Persona e Mercato*, 2: 279-296.
Tosi E. (2025). *Intelligenze artificiali e dati personali tra AI Act e GDPR: prime riflessioni su vulnerabilità digitale e crepuscolo del consenso*. In: *Dir. inf.*, 41(4-5): 681-731.
Vettori G. (2024). *Libertà e liceità del consenso nel trattamento dei dati. una premessa*. In: Orlando S., a cura di, *Libertà e liceità del consenso nel trattamento dei dati personali*. Firenze.
Viterbo F.G. (2008). *Protezione dei dati personali e autonomia negoziale*. Napoli.
Viterbo F.G. (2016). *Freedom of contract and the commercial value of personal data*. In: *Contr. impr./Eur.*, 21(2): 593-622.
Visintini G. (2019). *Dal diritto alla riservatezza alla protezione dei dati personali*. In: *Dir. inf.*: 1-20.
Warren S.D. e Brandeis L.D. (1890). *The Right to Privacy*. In: *Harvard Law Review*, 4(5): 193-220. DOI: 10.2307/1321160.
Zikesch P., Sörup T. e Adrian M. (2026). *Data Processing Service between Data Act and Digital Omnibus – A Term in Search of its Meaning*. In: *EuCML*, 1: 6-19.