RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 1/2026 • DOI 10.32091/RIID0276 • articolo sottoposto a peer review • pubblicato in anteprima il 4 giu. 2026

Laura La Corte

La natura relativa e contestuale della nozione di dato personale alla luce della sentenza *Deloitte*

Il contributo analizza l'evoluzione della nozione di dato personale alla luce della sentenza *Deloitte* del 4 settembre 2025, evidenziando come il tradizionale confine tra dato personale e dato anonimo risulti oggi sempre più incerto e labile. Muovendo dalla definizione ampia accolta dal GDPR, fondata sul criterio dell'identificabilità, si evidenzia come tale requisito non costituisca una qualità intrinseca dell'informazione, ma dipenda dal contesto, dai mezzi ragionevolmente utilizzabili e dalle finalità del trattamento. Particolare attenzione è dedicata alle tecniche di pseudonimizzazione e anonimizzazione, le quali mettono in crisi il tradizionale modello dicotomico tra dato personale e non personale. L'evoluzione delle tecnologie di analisi dei dati e dell'intelligenza artificiale accresce infatti il rischio di re-identificazione, mostrando come nessuna tecnica garantisca un'anonimizzazione assoluta. In questa prospettiva, la sentenza *Deloitte* segna un passaggio decisivo, affermando che la qualificazione giuridica di un dato può variare in base al contesto del trattamento e alle concrete possibilità di re-identificazione in capo al soggetto che lo tratta.Ne deriva la necessità di un modello di *governance* dinamico e fondato sul rischio, capace di bilanciare la tutela dei diritti fondamentali con le esigenze di circolazione dei dati nell'ecosistema digitale contemporaneo.

Dato personale – Identificabilità – Pseudonimizzazione – Anonimizzazione – Valutazione del rischio

The relative and contextual nature of the concept of personal data in the light of the *Deloitte* judgment

The article examines the evolution of the concept of personal data in light of the *Deloitte* judgment of September 4, 2025, highlighting how the traditional boundary between personal and anonymous data became increasingly blurred and uncertain. Drawing upon the broad definition adopted by the GDPR, based on identifiability, the author demonstrates that this requirement does not constitute an intrinsic property of information. Rather, it depends on the context, on the means reasonably likely to be used and on the purposes of the processing. The analysis focuses on pseudonymization and anonymization techniques, which challenge the traditional binary distinction between personal and non-personal data. The evolution of data analysis technologies and artificial intelligence indeed increases the risk of re-identification, proving that no technique can guarantee absolute irreversibility. In this regard, the Deloitte judgment marks a significant turning point by affirming that the legal data qualification may vary depending on the processing context and the concrete possibilities of re-identification available to the entity handling the data. This leads to the need for a dynamic, risk-based governance model capable of balancing the protection of fundamental rights and the necessity of data circulation within the contemporary digital ecosystem.

Personal data – Identifiability – Pseudonymisation – Anonymisation – Risk assessment

L'Autrice è dottoranda di ricerca in Discipline giuridiche pubblicistiche, curriculum Discipline pubblicistiche, internazionalistiche ed europee, presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre

Sommario: 1. La nozione di dato personale tra esigenze di innovazione e di tutela. – 2. La nozione dinamica di dato personale. – 3. Anonimizzazione e pseudonimizzazione dei dati: crisi del modello dicotomico. – 4. Conclusioni: verso un modello di governance dei dati basato sul rischio e sul contesto.

1. La nozione di dato personale tra esigenze di innovazione e di tutela

Il presente contributo si propone di indagare la nozione di dato personale muovendo dalla consapevolezza che il confine tra dato personale e dato anonimo fosse, fin dalla sua formulazione, intrinsecamente labile, posto che l'identificabilità non dipende solo dal contenuto dell'informazione ma dai mezzi concretamente impiegabili per ricondurla ad un individuo[1].

L'evoluzione tecnologica e le crescenti possibilità di re-identificazione ne hanno progressivamente accentuato la permeabilità[2]: la sentenza *Deloitte* del 4 settembre 2025[3] offre l'opportunità di analizzare un ulteriore momento di relativizzazione.

In tale contesto, la transizione digitale impone al giurista di confrontarsi con trasformazioni che, dissolvendo progressivamente i tradizionali confini tra sfera privata e spazio pubblico, incidono sul sistema di tutela dei diritti fondamentali.

Se, da un lato, l'impianto europeo appare costruito per garantire un'elevata protezione della persona anche in contesti tecnologicamente avanzati, dall'altro lato l'evoluzione delle tecniche di trattamento, fondate su capacità sempre più sofisticate di condivisione delle informazioni, mette alla prova la tenuta delle categorie giuridiche tradizionali[4].

Sullo studioso grava, quindi, il compito di verificare in quale misura il progresso tecnologico richieda l'elaborazione di nuove regole, oppure se le esigenze emergenti possano essere affrontate alla luce di regole e principi già applicati in materia di protezione dei dati personali[5].

La nozione ampia di dato personale accolta dal Regolamento generale sulla protezione dei dati personali[6] sembra offrire strumenti potenzialmente idonei ad accompagnare l'innovazione.

Tuttavia, l'espansione delle tecniche di profilazione induce a mettere in discussione la solidità della tradizionale distinzione tra dato relativo ad una persona identificata o identificabile e dato anonimo, specialmente considerando la "difficoltà tecnica di separare chirurgicamente i dati personali dai dati non personali"[7].

La possibilità tecnica di ricondurre, anche indirettamente, informazioni apparentemente neutre a una persona fisica impone di interrogarsi

1. Come già ampiamente rilevato in dottrina, cfr. *ex multis* D'Acquisto–Naldi 2017.
2. Come già ampiamente rilevato in dottrina, cfr. *ex multis* Calzolaio 2017.
3. Corte di giustizia Ue, sent. 4 settembre 2025, C-413/23 P.
4. Secondo il tradizionale insegnamento di Paolo Barile, infatti, "valgono regole opposte circa il segreto nel pubblico ed il segreto nel privato. L'apparato della democrazia ha per regola la trasparenza, ed il segreto costituisce una eccezione. I diritti costituzionalmente garantiti al soggetto privato in democrazia (la libertà nella comunità) hanno per regola la privacy, e per eccezione la pubblicità" (così Barile 1987, p. 29 ss.).
5. Passaglia 2016, p. 332.
6. Art. 4, n. 1 e, in particolare, cons. 26, Regolamento (UE) n. 2016/679 (GDPR).
7. Palmirani 2019, p. XII.

sull'efficacia delle misure di protezione previste e sulla capacità dell'ordinamento di prevenire i rischi di re-identificazione.

In questo scenario, un ruolo decisivo è svolto dalla Corte di giustizia dell'Unione europea[8], il cui intervento ha rafforzato la centralità dei diritti contenuti nella Carta dei diritti fondamentali dell'Unione europea che, proprio nel preambolo, evidenzia la necessità di "rafforzare la tutela dei diritti fondamentali, alla luce dell'evoluzione della società, del progresso sociale e degli sviluppi scientifici e tecnologici"[9].

Particolarmente significativa, in questo senso, è la sentenza *Deloitte*, laddove stabilisce che la qualificazione dei dati deve essere valutata in modo contestuale e relativo, non dipendendo solo dalla natura astratta dell'informazione ma tenendo conto dei mezzi effettivamente disponibili per il soggetto che li tratta.

In particolare, nella vicenda sottoposta al giudizio della Corte, i dati pseudonimizzati possono essere considerati anonimi per Deloitte, alla quale sono stati trasmessi senza l'accesso ai dati identificativi originari, e, dunque, nell'impossibilità concreta di re-identificare.

Di conseguenza, la valutazione dell'identificabilità va effettuata, ad avviso della Corte, al momento della raccolta dei dati e dal punto di vista del responsabile del trattamento.

Ciò solleva interrogativi di fondo: la pseudonimizzazione può rappresentare un punto di equilibrio sostenibile tra protezione e circolazione, o rischia di attenuare la responsabilità in caso di pericolo di re-identificazione? L'anonimizzazione è davvero compatibile con una tutela effettiva del dato personale in un ambiente digitale caratterizzato da una costante riaggregazione dei dati? È ancora adeguata una distinzione netta tra dato personale e dato non personale, oppure occorre ripensare in chiave graduale e dinamica il rapporto tra dato e persona?

È lungo queste direttrici, e alla luce della sentenza *Deloitte*, che si sviluppa la riflessione che segue, volta ad indagare la nozione di dato personale e a verificare se l'attuale impianto normativo sia ancora idoneo a garantire, nel contesto tecnologico attuale, una protezione effettiva dei diritti fondamentali senza sacrificare, al contempo, le esigenze di circolazione e valorizzazione dei dati.

2. La nozione dinamica di dato personale

Nell'attuale ecosistema digitale, il dato personale è in continua trasformazione, sospeso tra la tutela dell'identità individuale e la crescente valorizzazione economica dell'informazione[10].

La natura ambivalente del dato personale[11], in quanto oggetto di un diritto fondamentale e bene di valore economico, determina una tensione tra la circolazione dei dati e la protezione degli stessi, concepita non come un fine assoluto, bensì come uno strumento di tutela degli interessi, di volta in volta, sottostanti.

Nonostante la recente spinta verso la condivisione e apertura dei *big data*, a beneficio del mercato e della collettività, la disciplina del GDPR, focalizzandosi sui dati a carattere personale, mostra la scelta assunta dal legislatore, al bivio tra i due interessi in gioco: la protezione dei dati – ovvero la protezione di un diritto fondamentale sancito dalla Carta europea dei diritti fondamentali (art. 8) – prima della circolazione[12].

Tuttavia, di fronte al necessario sviluppo delle tecnologie digitali, è opportuna una riflessione anche sui dati non personali, categoria residuale e limitata in modo significativo dalla natura ampia e mutevole del concetto stesso di dato personale.

Il macro-ambito della nozione di dato, comprende, infatti, oltre ai dati personali, anche i dati non personali, la cui residualità emerge dalla definizione "negativa" offerta dall'art. 3, punto 1, del Regolamento UE 1807/2018[13], come "dati diversi

8. Sull'impatto della giurisprudenza della Corte di giustizia v. Amalfitano–Ferri 2023, p.17 ss.
9. Preambolo della Carta dei diritti fondamentali dell'Unione europea.
10. Sul valore e la circolazione dei dati v. Cremona–Laviola–Pagnanelli 2022; Nicita 2019.
11. Faini 2023, p. 388.
12. Torregiani 2020, p. 319; Montagnani 2019, p. 15.
13. Regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea del 14 Novembre 2018.

dai dati personali definiti dall'art. 4, punto 1, del Regolamento (UE) 2016/679".

La problematicità della differenziazione tra dati personali e non personali emerge con particolare evidenza se si guarda non solo alla qualificazione del dato, ma anche allo statuto giuridico che l'ordinamento europeo riconosce alle due categorie, comportando l'applicazione di discipline diverse proprio sotto il profilo della circolazione, dell'accessibilità e del trasferimento verso Paesi terzi.

Mentre i dati personali sono sottoposti al sistema di garanzie del GDPR, fondato sui principi di liceità, minimizzazione, limitazione delle finalità, *accountability* e sulle rigorose condizioni previste dagli artt. 44 ss. per i trasferimenti internazionali, i dati non personali sono invece assoggettati, in linea di principio, ad un regime ispirato alla libera circolazione, come espressamente previsto dal Regolamento (UE) 2018/1807, che vieta restrizioni alla localizzazione dei dati all'interno dell'Unione salvo esigenze di sicurezza pubblica.

La dicotomia tra dato personale e non personale, continuamente messa in discussione da strumenti volti a rilevare "connessioni 'invisibili' tra i dati"[14] per ricavare nuove informazioni, determina il campo di applicazione del GDPR. Di conseguenza, è proprio nell'interpretazione dell'art. 4, che si individua il suo ambito di operatività.

La definizione fornita dall'art. 4 del GDPR, rimasta immutata rispetto alla Direttiva 95/46, qualifica il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)"[15].

Risulta evidente che la disciplina della protezione dei dati si fonda sull'interazione di quattro elementi chiave, in cui è possibile scomporre la definizione. Il primo è il riferimento a "qualsiasi informazione"; il secondo è l'aggettivo verbale "riguardante"; il terzo, l'espressione "una persona fisica"; infine, la caratteristica di "identificata o identificabile"[16].

Per cogliere l'effettiva portata della nozione di dato personale è, dunque, necessario analizzare i suddetti aspetti fondamentali, poiché è proprio il concetto di identificabilità che, tradizionalmente, traccia la linea di confine tra quanto è soggetto alla normativa del GDPR e ciò che, invece, non rientra nel suo ambito di applicazione.

Emerge, anzitutto, la scelta di un linguaggio onnicomprensivo, che, offrendo il vantaggio di abbracciare con lungimiranza anche le situazioni nuove e non prevedibili dal legislatore, originate dalla rapida e continua evoluzione del mondo digitale, è sintomo di una sempre maggiore presa di coscienza della "eccedenza della vita rispetto alle regole"[17].

La scelta lessicale dell'espressione "qualsiasi informazione", che apre la disposizione, è il primo

14. Torregiani 2020, p. 318.

15. Iinterviene sulla nozione di dato personale sancita dall'art. 4, par. 1, GDPR la Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e le direttive 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 per quanto riguarda la semplificazione del quadro legislativo nel settore digitale e che abroga i regolamenti (UE) 2018/1807, (UE) 2019/1150 e (UE) 2022/868 e la direttiva (UE) 2019/1024 (omnibus digitale). L'articolo 3, *Modifiche del Regolamento (UE) 2016/679* (GDPR) stabilisce, infatti, che "l'articolo 4 è così modificato: (a) al punto 1) sono aggiunte le frasi seguenti: le informazioni relative a una persona fisica non sono necessariamente dati personali per qualsiasi altra persona o entità per il solo fatto che un'altra entità può identificare tale persona fisica. Le informazioni non sono personali per una determinata entità se quest'ultima non è in grado di identificare la persona fisica cui si riferiscono le informazioni, tenendo conto dei mezzi di cui tale entità si può ragionevolmente avvalere. Tali informazioni non diventano personali per tale entità per il solo fatto che un potenziale destinatario successivo dispone di mezzi di cui si può ragionevolmente avvalere per identificare la persona fisica cui le informazioni si riferiscono". Il *Digital Omnibus Package*, inserendosi nel contesto di una complessiva strategia di razionalizzazione avviata dopo il rapporto di Mario Draghi sul futuro della competitività europea, orientata a semplificare la normativa digitale per sostenere la crescita industriale e il progresso tecnologico, accoglie una qualificazione di dato personale che non deriverebbe da una valutazione oggettiva della natura dell'informazione, bensì dipenderebbe dalle caratteristiche specifiche del soggetto che ne è in possesso.

16. Bolognini–Bistolfi 2016, p. 4.

17. Colapietro 2018, p. 16.

indice dell'elasticità che permea la definizione di dato personale, in quanto, lungi dall'essere una formulazione generica, è una precisa scelta normativa, volta ad attribuire alla nozione di dato personale una portata ampia, tale da ricomprendere ogni elemento informativo che, direttamente o indirettamente, possa riguardare una persona fisica.

Nella consapevolezza che l'identità di un individuo può emergere da una pluralità di informazioni, anche apparentemente neutre o frammentarie, si consente, così, alla definizione di operare anche a fronte di dati generati da nuovi strumenti digitali e di tutelare l'integrità della persona nel mutevole ecosistema digitale contemporaneo.

In particolare, nel recepire gli orientamenti contenuti nel Parere n. 4/2007 del Gruppo *ex* art. 29[18], la nozione di dato personale si ritiene onnicomprensiva tanto dal punto di vista della natura dell'informazione (sia essa soggettiva, oggettiva, veritiera o meno) quanto sotto il profilo del contenuto (relativo a dati generali e sensibili), ma anche in riferimento alla forma (indipendentemente dal supporto utilizzato, che sia cartacea, numerica, alfabetica, fotografica o sonora).

L'ampiezza della formulazione fin qui esaminata è, tuttavia, ristretta dal successivo requisito richiesto affinché si possa parlare di dato personale: che l'informazione sia "riguardante" l'interessato, cui il dato si riferisce.

In particolare, per considerare un dato riguardante un individuo, devono sussistere tre caratteristiche alternative[19].

Il primo criterio è la presenza di un elemento di contenuto, che ricorre quando, dal contenuto stesso dei dati, è possibile identificare direttamente una persona fisica, indipendentemente dalle finalità del trattamento. In altre parole, l'informazione concerne chiaramente un individuo: ad esempio, un referto medico che indica il nome del paziente[20].

Il secondo elemento, quello della finalità, ricorre quando, anche in assenza di un collegamento diretto tra i dati e la persona fisica, lo scopo del trattamento è tale da influenzare lo status o il comportamento dell'interessato. Un esempio è rappresentato dai registri chiamate di un'azienda: a seconda della finalità del trattamento, i dati possono riferirsi ai dipendenti o ai clienti. Dunque, è l'obiettivo per cui i dati vengono trattati a determinare a chi essi si riferiscono.

Infine, l'elemento del risultato si riferisce ai casi in cui il trattamento dei dati produce effetti nella sfera giuridica o personale dell'interessato. Ad esempio, un sistema di localizzazione che assegna automaticamente una corsa al tassista più vicino al cliente può generare informazioni sul comportamento del conducente stesso, come i percorsi abituali, producendo, così, effetti sulla sua attività professionale[21].

La dinamicità della nozione di dato personale[22] è rafforzata dall'interpretazione di persona "identificabile", da tenere distinta rispetto a quella "identificata". Infatti, un individuo è identificato quando è distinto in modo certo da tutti gli altri membri di un gruppo. Sarà, invece, identificabile quando, pur non essendo ancora stato identificato, esistono elementi significativi grazie ai quali si può risalire, direttamente o indirettamente, alla sua identità, restringendo sempre più il gruppo al quale appartiene[23].

Nonostante l'estensione dell'espressione, rintracciamo delle linee guida interpretative nei considerando 26 e 30 del GDPR.

Il primo sottolinea che "per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi" valutando "l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici". Si noti qui l'utilizzo dell'avverbio "ragionevolmente", che orienta

18. Data Protection Working Party (WP29), *Parere 4/2007 sul concetto di dati personali.*

19. Stalla-Bourdillon–Knight 2017; Di Resta 2018, p. 8 s.

20. Rientrano in questa categoria non solo i nomi, ma anche gli identificatori univoci, come un numero di passaporto, che consente di risalire in modo inequivocabile all'interessato.

21. Sui criteri esaminati cfr. anche Lee Bygrave–Docksey–Kuner 2020 e Riccio–Scorza–Belisario 2018.

22. Cfr. la tesi espressa in dottrina da Colapietro–Iannuzzi 2017 e Calzolaio 2017.

23. Bolognini–Bistolfi 2016, p. 4.

verso una concezione ampia di dato personale, a supporto del modello finora descritto[24].

Il secondo considerando citato chiarisce che, sempre ai fini dell'identificabilità "le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

Tale disposizione è la codificazione degli approdi raggiunti dalla giurisprudenza della Corte di giustizia, in particolare con la sentenza *Breyer*[25], in cui l'indirizzo IP dinamico[26] di un utente di un sito web è stato considerato un dato personale[27], in base alle informazioni detenute dal provider di accesso a internet.

Infatti, la possibile combinazione degli indirizzi IP con le informazioni degli abbonati del fornitore del servizio Internet consentirebbe di identificare in modo certo l'utente e configurare, dunque, un dato personale, per scopo o per risultato, essendo, in qualche modo, assimilabile a un dato di localizzazione[28]. Pertanto, per determinare se gli indirizzi IP costituiscano dati personali, è fondamentale considerare quali informazioni vengono associate ad essi e gli scopi per cui i dati sono trattati, poiché è la combinazione di diversi identificatori a consentire il passaggio dall'essere una persona identificabile all'essere una persona identificata, risultando necessaria una valutazione basata sul contesto.

L'esame dei casi concreti, evidenzia, infatti, una certa complessità nel definire un criterio uniforme di identificabilità, portando a preferire un approccio di tipo relativo.

Una simile impostazione, che valorizza il contesto d'uso del dato più che la sua natura ontologica, trova un interessante parallelismo nel diritto cinese, che distingue concettualmente tra *personal information* e *data*, attribuendo alle due nozioni un differente statuto giuridico in base alla funzione che assolvono e agli interessi che vengono in rilievo[29].

Da un lato, la nozione di *personal information*, accolta dal *Personal Information Protection Law* (PIPL), rileva quando l'informazione sia idonea a incidere sui diritti ed interessi della persona fisica; dall'altro, la nozione di *data*, presente nel *Data Security Law* (DSL) e nel *Cybersecurity Law* (CSL), assume rilievo quando l'interesse in gioco sia l'interesse pubblico, quale risorsa strategica per la sicurezza e la sovranità digitale dello Stato.

L'adozione della nozione di informazione in luogo di quella di dato comporta rilevanti conseguenze sul piano giuridico, poiché sposta l'attenzione dalla dimensione ontologica del dato al suo profilo funzionale.

In questa prospettiva, ai fini dell'applicazione della disciplina in materia di protezione dei dati personali, rileva la concreta possibilità che il titolare del trattamento utilizzi i dati per ricavare informazioni riferibili ad una persona fisica. Ne consegue che, ai fini della tutela della persona, la nozione di informazione personale consente meglio di calibrare l'applicazione delle garanzie normative alle effettive caratteristiche del trattamento e del rischio per l'interessato.

Una simile articolazione di categorie suggerisce la possibilità di superare anche in Europa la tradizionale e piuttosto semplice distinzione tra dati personali e dati non personali, in favore di

24. Di Resta 2018, p. 14.

25. Corte di giustizia Ue, sentenza in causa C-582/14, *Patrick Breyer vs Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

26. Un indirizzo IP dinamico è un indirizzo che cambia ad ogni connessione Internet e viene assegnato automaticamente a un dispositivo quando si connette a una rete.

27. Cf. ENISA, *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*, November 2019, in cui gli indirizzi IP, insieme agli indirizzi e-mail, vengono analizzati come casi d'uso di pseudonimizzazione.

28. Stalla-Bourdillon–Knight 2017.

29. Calzolaio 2023.

una disciplina più idonea all'era contemporanea dell'IA e della datificazione.

È alla luce di tali considerazioni che va letto il primo motivo di decisione della Corte di giustizia nella sentenza *Deloitte*, laddove stabilisce che "la natura particolare delle opinioni e dei pareri personali (…) in quanto espressione del pensiero di una persona, sono necessariamente strettamente legati a quest'ultima"[30]. Non era, pertanto, necessario, in tal caso, un esame del contenuto, scopo o effetti dei commenti rilasciati dagli azionisti alla SRB, risultando pacifico che fossero espressione degli autori e, quindi, dati personali.

L'interpretazione adottata dalla Corte è supportata dalla sentenza del 20 dicembre 2017, Nowak (C-434/16), in cui, in riferimento ai commenti di un esaminatore sulle prove scritte di un candidato in sede di esame, si rilevava che gli stessi riflettono inevitabilmente la personale valutazione dell'esaminatore e sono, dunque, a quest'ultimo riferibili.

Si legge, infatti, in tale pronuncia, che "l'uso dell'espressione 'qualsiasi informazione' (…) riflette l'obiettivo del legislatore dell'Unione di attribuire un'accezione estesa a tale nozione, che non è limitata alle informazioni sensibili o di ordine privato, ma comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano "concernenti" la persona interessata"[31] [32].

3. Anonimizzazione e pseudonimizzazione dei dati: crisi del modello dicotomico

Se l'identificabilità rappresenta il criterio cardine per l'applicazione del GDPR, occorre allora interrogarsi su quali siano gli strumenti tecnici e giuridici attraverso i quali il legislatore europeo la attenua o esclude. È in questa prospettiva che si inseriscono le tecniche di anonimizzazione e pseudonimizzazione dei dati[33], nonché la sentenza *Deloitte*, nell'affermare che "i dati pseudonimizzati non devono essere considerati come costituenti, in tutti i casi e per ogni persona, dati personali ai fini dell'applicazione del regolamento 2018/1725, nella misura in cui la pseudonimizzazione può, a seconda delle circostanze del caso, impedire effettivamente a persone diverse dal responsabile del trattamento di identificare l'interessato in modo tale che, per loro, l'interessato non sia o non sia più identificabile"[34].

Il considerando 26 del GDPR stabilisce che il Regolamento non si applica al trattamento di informazioni anonime, "vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato"[35]. Tali tecniche trovano applicazione sia nella conservazione dei dati sia nella loro eventuale comunicazione a terzi, in particolare in ambiti di natura statistica, storica o scientifica.

Al contrario, il GDPR si applica integralmente ai dati pseudonimizzati, in quanto, pur essendo sottoposti a tecniche di riduzione dell'identificabilità, conservano la qualificazione di dati personali.

La pseudonimizzazione[36] è definita all'art. 4 del GDPR come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e

30. Corte di giustizia Ue, sent. 4 settembre 2025, C-413/23 P.
31. Corte di giustizia Ue, sent. 20 dicembre 2017, *Nowak*, C-434/16.
32. Assume rilievo, in questo quadro, la clausola contenuta nel primo comma dell'art. 21 Cost., inserita con lungimiranza, lì dove prevede la possibilità di esercitare la libertà di pensiero con "ogni mezzo di diffusione", così da garantire nuove forme di tutela costituzionale anche a nuove forme di espressione, frutto dell'evoluzione delle moderne tecnologie. Analogamente, l'art. 15 Cost. prevede, al primo comma, che "la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili".
33. D'Acquisto–Naldi 2017.
34. Corte di giustizia Ue, sent. 4 settembre 2025, C-413/23 P., punto 86.
35. Reg. UE 679/2016, considerando 26.
36. Gabel–Schiering 2018; EDPB, *Guidelines 01/2025 on Pseudonymisation*.

organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

Tale definizione è al tempo stesso restrittiva e molto ampia. È restrittiva nella misura in cui non comprende i processi di trattamento che non riescano a garantire l'attribuzione dei dati personali a una persona fisica identificabile. Dall'altro lato, è una definizione ampia, in quanto non richiama la collegabilità dei dati come problema fondamentale alla base del rischio che gli individui possano ancora essere individuati, anche dopo l'applicazione di tecniche di pseudonimizzazione[37].

In particolare, maggiore è la quantità di informazioni relative ad un individuo, maggiore è la probabilità che queste vengano impiegate per identificarlo o per ottenere dati a lui riferibili. Il rischio di re-identificazione è legato, quindi, all'aggregazione, ovvero la combinazione di dati, tale da generare una nuova informazione.

Si pensi che uno studio condotto dalla professoressa Latanya Sweeney[38] dimostra che la combinazione di un codice postale, della data di nascita e del genere è sufficiente a identificare l'87% degli individui negli Stati Uniti. Questo perché i dati non personali non esistono mai isolati ma sono parte di un insieme dinamico di informazioni disponibili per ogni individuo[39].

Il Parere 5/2014 del Gruppo di Lavoro Art. 29[40], a tal proposito, fa riferimento alla necessità di valutare molteplici fattori in costante evoluzione, che contribuiscono al contesto in cui le tecniche di de-identificazione operano, quali lo stato della tecnologia, le finalità del trattamento, la disponibilità di informazioni ulteriori, evidenziando la presenza di un "rischio intrinseco residuo di reidentificazione"[41] tale che "nessuna tecnica è di per sé esente da carenze"[42].

Per questi motivi, l'Agenzia dell'Unione europea per la cybersicurezza (ENISA) ha contribuito a individuare una serie di principi generali di progettazione che ogni titolare del trattamento dovrebbe considerare nella scelta delle tecniche di pseudonimizzazione[43].

Il primo obiettivo ivi previsto è quello di garantire che lo pseudonimo non consenta facilmente a terzi di re-identificare. Verificato questo aspetto, il titolare deve adottare misure che impediscano a terzi di riprodurre gli stessi pseudonimi.

È bene, però, tenere presente che non è possibile eliminare del tutto il rischio di re-identificazione degli individui[44].

In quest'ottica, diventa fragile il confine tra dati personali e dati anonimi, la cui dicotomia è fondata su un approccio statico legato ad una qualità intrinseca del dato. Al contrario, lo stato dei dati sottoposti a misure di pseudonimizzazione e, ancor di più, a misure di anonimizzazione, deve essere valutato in modo dinamico, alla luce del contesto e mediante monitoraggi continui, poiché, nell'impossibilità di tracciare un vademecum valido in ogni caso, è necessario adottare un approccio orientato al rischio[45].

Infatti, tra le critiche sollevate, in particolare nei confronti della "anonimizzazione come una sorta di panacea di tutti i mali"[46], che consente al titolare del trattamento di liberarsi dalle maglie del GDPR, assume rilievo quella di Paul Ohm[47]. Egli

37. Stalla-Bourdillon–Knight 2017, p. 17 s.
38. Sweeney 2000.
39. In questi termini Schwartz–Solove 2011, p. 1843.
40. Gruppo di Lavoro Art. 29 per la protezione dei dati, *Parere 05/2014 sulle tecniche di anonimizzazione (WP216, 0829/14/IT),* 10 aprile 2014 [di seguito Parere 05/2014].
41. Parere 05/2014, p. 7.
42. *Ivi*, p. 12.
43. ENISA, *Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation,* November 2018; ENISA, *Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions*, November 2019.
44. *Ibidem*. V. anche Trovato–Rauccio 2022.
45. Foglia 2019, p. 311 ss.
46. *Ivi*, p. 310.
47. Ohm 2010.

sostiene che l'anonimizzazione di tipo "*release and forget*" è una promessa illusoria e propone di abbandonare la tradizionale distinzione tra dati personali e non personali, attraverso una valutazione dei rischi concreti di re-identificazione, più aderente alla realtà.

In un simile ripensamento del paradigma, così proposto da Ohm, sarebbe necessario considerare le molteplici sfumature di "identificabilità" comprese tra i due poli dei dati riferibili a soggetti identificati e quelli anonimi poiché non è possibile escludere con certezza la possibilità di re-identificare un dato reso anonimo.

Lo sviluppo delle tecniche di analisi dei dati e la crescente diffusione delle politiche di *open access* rendono, infatti, sempre più irrealizzabile un'anonimizzazione rigorosa, così che l'irreversibilità non è più un requisito assoluto, ma un obiettivo cui il titolare del trattamento deve tendere, al fine di ridurre il rischio entro termini accettabili[48]. In sostanza, un dato che oggi non è personale potrebbe diventarlo in futuro, in quanto l'identificabilità dipende dal contesto.

È stato osservato come l'evoluzione tecnologica potrebbe condurre a trasformare il diritto alla protezione dei dati personali in un "law of everything"[49], poiché un numero sempre più crescente di dati sarà potenzialmente riconducibile alla nozione di dato personale e, conseguentemente, assoggettato all'ambito di applicazione del GDPR.

In ecosistemi digitali sempre più "intelligenti", infatti, ogni informazione può potenzialmente essere ricondotta, direttamente o indirettamente, a una persona fisica.

Ciò non significa accettare la tesi di Ohm secondo cui "data can be useful or perfectly anonymous but not both"[50] che, se presa alla lettera, condurrebbe ad un disincentivo nell'uso delle misure di anonimizzazione[51]. Il fatto che non sia possibile eliminare in modo assoluto il rischio di re-identificazione, non implica la mancanza di utilità di tali tecniche che, sebbene non garantiscano l'eliminazione del rischio, lo riducono ragionevolmente, in linea con l'altro grande principio del GDPR: quello della valutazione, che spetta al titolare svolgere, finalizzata alla riduzione in concreto dei rischi per i diritti dell'interessato (cd. *risk based approach* e *accountability*).

Di conseguenza, dipenderà dal contesto la definizione stessa di dato personale poiché, se l'anonimizzazione non è una caratteristica intrinseca del dato, neppure la personalizzazione (cioè la qualificazione del dato come personale) può essere considerata proprietà del dato in quanto tale. Essa deve essere piuttosto riferita al contesto in cui il dato è inserito, in quanto, sebbene l'identificabilità sia un elemento chiave nella definizione di dato personale, non è l'unico da tenere in considerazione[52].

Per "contesto" si intendono, infatti, la finalità (concreta) del trattamento e, dunque, l'intenzione del titolare del trattamento, ma anche gli utilizzi attuali e potenziali, ad esempio, mediante future combinazioni con altri tipi di dati che il titolare è in grado effettivamente di mettere in atto.

In particolare, l'ambiente dei dati si può ritenere composto da quattro elementi chiave[53]: il primo sono gli "altri dati", cioè i dati con cui il dato anonimizzato può entrare in connessione; il secondo elemento sono gli utenti dei dati che, in seguito alla condivisione dei dati, li analizzano, trasformano, combinano con altre informazioni; il terzo elemento è relativo ai processi di governance che regolano le relazioni tra utenti e dati; infine, l'infrastruttura, composta da sistemi fisici e software che controllano l'accesso e l'interazione con i dati.

Dunque, la linea di demarcazione tra dati personali e non personali è fluida e può mutare nel tempo, determinando la possibilità che i dati anonimizzati al tempo t1 diventino nuovamente dati personali al tempo t2, considerando che, una volta che i dati confluiscono nell'oceano digitale, è sempre più difficile contenere il rischio di re-identificazione.

48. Torregiani 2020, p. 325.
49. Finck–Pallas 2020, p. 20.
50. "I dati possono essere utili o perfettamente anonimi, ma non entrambi", Ohm 2010.
51. Elliot–O'Hara–Raab et al. 2018, p. 10.
52. Stalla-Bourdillon–Knight 2017, p. 28 s.
53. Elliot–O'Hara–Raab et al. 2018, p. 17.

D'altra parte, prevedere la distruzione di un dataset correttamente anonimizzato risulta essere un obbligo troppo stringente in capo al titolare del trattamento, poiché ne risentirebbe il flusso di dati, la cui fruizione è essenziale in settori basati proprio sull'analisi e la conservazione dei dati stessi (c.d. *data driven innovation*).

Se l'obiettivo è quello di agevolare la circolazione dei dati, occorre allora adottare una prospettiva diversa, che tenga conto non solo del dato in sé, ma anche del soggetto che lo tratta e del relativo contesto.

In alternativa all'approccio tradizionale, è stato infatti proposto un modello basato sull'uso dei dati (*use model*)[54] in cui si sposta il focus dalla fase di raccolta dei dati a quella del loro utilizzo. L'idea alla base è che il momento in cui tali dati vengono effettivamente impiegati determina rischi e benefici, i quali devono guidare le decisioni sull'utilizzo, tenendo conto del centrale elemento del contesto.

Questo approccio tende a ridurre l'attenzione sulla distinzione tra dati personali e non personali, concentrandosi piuttosto sugli effetti concreti che l'uso delle informazioni può produrre sugli individui.

In tale ottica, il soggetto terzo a cui venga trasferito un dataset anonimizzato entrerebbe in possesso di un insieme di dati da considerarsi per lui anonimi, in riferimento ai quali, pertanto, non assumerebbe la qualifica di titolare del trattamento, in quanto il GDPR non troverebbe applicazione.

A seconda del punto di vista adottato, il medesimo dato potrebbe avere natura diversa e, per l'appunto, dinamica: per il titolare originario, che conserva la disponibilità del dataset autentico ed è in grado di risalire all'identità degli interessati, le informazioni "anonimizzate" continuano ad essere dati pseudonimizzati, e quindi personali; al contrario, per il soggetto terzo, tale dato può assumere natura effettivamente anonima, e quindi non personale, qualora il contesto del trattamento comporti un rischio di re-identificazione inferiore alla soglia di accettabilità[55].

Il quadro descritto viene recepito anche dal GDPR che, a prima vista, sembra mantenere netta la distinzione tra dati anonimi e pseudonimizzati/personali. Tuttavia, una lettura più attenta rivela, "tra le righe", la possibilità di individuare una fascia di dati intermedia, comprensiva di diversi livelli di identificabilità cui corrispondono più gradazioni di rischio e, di conseguenza, obblighi di intensità diversa per i titolari del trattamento.

In particolare, l'art. 11 stabilisce che "se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente Regolamento", coerentemente con il principio di minimizzazione. L'articolo prosegue affermando che "qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione".

Siamo davanti, quindi, a dati personali – che, nel corso del trattamento, vengono pseudonimizzati fino a lambire l'anonimizzazione per il titolare – che perdono progressivamente il carattere dell'identificabilità per il titolare stesso, il quale non può operare il collegamento con la persona fisica, a meno che non gli vengano fornite *ex novo* informazioni aggiuntive. Pertanto, i diritti dell'interessato previsti dagli articoli da 15 a 20 del GDPR, in assenza di tali ulteriori informazioni, non troveranno oggetto (cioè i dati personali) per la loro applicazione.

Così, anche l'impiego di misure di pseudonimizzazione può, a seconda del contesto, generare dati collocabili in gradini diversi della scala di identificabilità, a ognuno dei quali si associa un diverso grado di re-identificazione e da cui, in ultima analisi, consegue l'applicazione o meno del GDPR[56].

Si noterà che questa impostazione ha un effetto significativo: i titolari del trattamento sarebbero davvero incentivati a percorrere la via di una pseudonimizzazione seria e sistematica, poiché ciò implica una loro minor esposizione a responsabilità

54. OCSE, *Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*, 21 March 2014, p. 14 ss.

55. In questi termini Torregiani 2020, p. 328.

56. In questi termini anche Irti 2022, p. 53 ss.

giuridica. Ne deriverebbe, su larga scala, una tutela più efficace dei diritti e delle libertà degli interessati.

4. Conclusioni: verso un modello di governance dei dati basato sul rischio e sul contesto

La sentenza *Deloitte* costituisce un punto di snodo nel percorso di progressiva relativizzazione della nozione di dato personale, ponendo in evidenza come l'identificabilità non sia una qualità intrinseca dell'informazione, bensì il risultato di una valutazione che dipende dal contesto del trattamento e dai mezzi concretamente disponibili in capo al soggetto che tratta i dati.

Nel riconoscere che un dato pseudonimizzato possa assumere natura diversa a seconda del destinatario e delle sue capacità di re-identificazione, la Corte di giustizia prende definitivamente le distanze da una concezione statica e assoluta del dato, aprendo la strada ad un modello fondato sulla relazione tra dato e informazione personale, tra soggetto e ambiente tecnologico.

Tale approdo giurisprudenziale si inserisce in un ecosistema digitale in cui il dato tende a perdere il proprio ancoraggio all'oggetto materiale, soprattutto nei contesti di *cloud computing* che dematerializzano i dati in luoghi virtuali e rendono difficile il diretto controllo dell'interessato[57].

In tale quadro, il dato personale non coincide con un bene di cui il soggetto dispone, ma rappresenta una proiezione della persona nello spazio pubblico digitale, con il rischio di "un'intimità (…) sradicata"[58], che richiede all'utente di non essere relegato al ruolo di mero spettatore del contesto digitale in cui è immerso ma di esercitare la propria autodeterminazione informativa[59].

Tuttavia, è necessario muovere dalla consapevolezza che l'individuo non è più in grado di mitigare i nuovi potenziali rischi attraverso i tradizionali strumenti di tutela basati sul consenso e sull'autodeterminazione, in quanto "i dati generano altri dati"[60], sempre più spesso creati senza il diretto coinvolgimento dell'individuo stesso.

Da qui discende la necessità di ripensare il valore da riconoscere alle tecniche di anonimizzazione e pseudonimizzazione dei dati al fine di valorizzare una protezione efficace dei dati personali e di accettare una governance dinamica del GDPR[61].

Come evidenziato, la tradizionale concezione dell'anonimizzazione come "stato del dato"[62] e strumento idoneo a recidere il legame tra dato e persona appare da tempo insufficiente se non accompagnata da una valutazione contestuale e dinamica del rischio di re-identificazione[63].

La nozione stessa di dato anonimo risulta problematica, generando l'illusione di un confine definitivo tra dati personali e non personali che, nella realtà tecnologica contemporanea, risulta sempre più difficile da sostenere[64]. Per questa ragione, il criterio fondato sul rischio accolto dal considerando 26 del GDPR sembra rappresentare il parametro più idoneo.

57. Galiano–Leogrande–Massari–Massaro 2020, p. 63. Sui diritti dell'interessato v. Calisai 2019, p. 327 ss.; Colapietro–Iannuzzi 2017, p. 85 ss.
58. Esposito 2021, p. 498.
59. Sul fondamentale ruolo del consenso v. Caggia 2019, p. 249 ss.; Colapietro–Iannuzzi 2017, p. 85 ss.
60. Abrams 2014, p. 9.
61. Si individuano quattro modelli emergenti di governance dei dati che rappresentano diverse configurazioni del rapporto tra dato, attori e ambiente tecnologico: le *Data Sharing Platforms* (DSP), cioè iniziative tra titolari di dati, che aggregano dati provenienti da fonti diverse per creare maggiore valore attraverso la loro combinazione; le *Data Cooperatives* (DC), che introducono una dimensione maggiormente partecipativa, in cui i soggetti dei dati assumono un ruolo attivo nella gestione collettiva delle informazioni; *Public Data Trusts* (PDT), in cui è il soggetto pubblico ad assumere il ruolo di fiduciario dei dati. In questo caso, la governance si basa su un rapporto di fiducia istituzionalizzata tra cittadini ed enti pubblici, con l'obiettivo di garantire un uso etico e orientato al bene comune dei dati; *Personal Data Sovereignty* (PDS), che attribuisce ai soggetti dei dati un controllo diretto sulle proprie informazioni attraverso spazi personali dei dati. Sul punto v. Micheli–Ponti–Craglia–Berti Suman 2020.
62. Bolognini–Bistolfi 2016, p. 2.
63. Cfr. Viola De Azevedo Cunha–Doneda–Andrade 2010, pp. 641-655.
64. Finck–Pallas 2020, p. 20.

Di conseguenza, i titolari del trattamento sono chiamati a garantire un livello di sicurezza adeguato e ad effettuare periodiche valutazioni del rischio di identificabilità, alla luce dei mezzi ragionevolmente utilizzabili dal titolare del trattamento ma anche dal terzo a cui vengono trasferiti i dati, poiché le sue caratteristiche e il suo ambiente tecnologico incidono sulla possibilità di re-identificazione[65].

Tale dovere di monitoraggio impone di "superare il modello del *release and forget* o, ancor meglio, quello del *release and complete freedom*"[66] a favore di una maggior responsabilizzazione effettiva degli attori coinvolti nella circolazione dei dati, inclusi i destinatari di dataset formalmente anonimizzati, i quali non possono ritenersi del tutto estranei alla disciplina del GDPR, anche se non sono (ancora) titolari del trattamento.

Questo approccio consente, da un lato, di salvaguardare la circolazione delle informazioni, in quanto la qualificazione di un dataset come anonimo, e dunque come dato non personale, non comporta soltanto l'uscita dall'ambito applicativo del GDPR, ma produce un effetto di vera e propria "liberalizzazione regolatoria", consentendo una circolazione significativamente più ampia del dato, anche in contesti globali di *cloud computing, data sharing* e sviluppo di sistemi di intelligenza artificiale, favorendo, così, il riutilizzo dei dati[67]; dall'altro, permette di modulare il livello di tutela in funzione dei rischi concreti per gli interessati, conducendo ad una concezione graduale del dato, a beneficio della ricerca scientifica, dello sviluppo di algoritmi di intelligenza artificiale e, più in generale, di molte aziende, per le quali si apre una nuova stagione di *compliance*, orientata ad una conformità alla legge non più passiva ma proattiva.

In altri termini, la nozione dinamica di dato personale ha il carattere della reversibilità: se da un lato, il dato pseudonimizzato può essere anonimo – e quindi non personale – per un terzo soggetto che lo tratta e non è in grado di identificare il potenziale interessato, dall'altro, se un soggetto che tratta dati anonimi è materialmente in grado di re-identificare l'interessato, allora il "dato" riacquisisce il suo carattere "personale" e quel terzo diventa un titolare/responsabile del trattamento cui si applica il GDPR.

A tal fine, i titolari del trattamento e, fra questi, in modo particolare le imprese dovranno guidare l'innovazione, secondo una modalità che tende a valorizzare il ruolo centrale del DPO, attraverso solidi programmi di governance che richiedono di mappare i flussi e il regime tecnico dei dati, integrare le nuove tecnologie (come l'IA) e applicare con attenzione e lungimiranza le misure di pseudonimizzazione e anonimizzazione, in modo da poter dimostrare, in ogni momento, che il titolare non persegue, quale finalità del trattamento, l'identificazione delle persone fisiche e, di conseguenza, adotta misure idonee ad impedirne l'identificazione.

La prospettiva adottata dalla Corte di giustizia nella sentenza *Deloitte* si presta, dunque, ad essere letta come espressione di una più ampia evoluzione del diritto alla protezione dei dati personali, mostrando come sia sufficiente cambiare lo sguardo sulle norme già esistenti del GDPR, in quanto quest'ultimo è in grado di adattarsi all'innovazione tecnologica mediante i criteri di ragionevolezza e bilanciamento.

Anche le autorità di *data protection* dovranno ora tenere conto di questa nuova lettura del dato normativo, che supera la distinzione "scolpita nella pietra" tra dato anonimo e dato personale e apre la strada ad un modello di protezione dei dati fondato sulla responsabilizzazione del soggetto che tratta i dati, quando questi sono effettivamente personali, e su una valutazione elastica, orientata dall'uso in concreto delle informazioni personali.

Si tratta, in ultima analisi, di un orientamento non distante da un' impostazione che valorizza il principio di lealtà nel trattamento dei dati personali e che sembra farsi strada anche nella dottrina di oltreoceano[68].

65. Elliot–O'Hara–Raab et al. 2018 propongono una "anonimizzazione funzionale", cioè un approccio che considera anche l'ambiente di trattamento del dataset e che richiede al titolare del trattamento di progettare tale ambiente, prevedendo chiare responsabilità in relazione alla comprensione dei rischi, alla predisposizione di controlli di accesso e di un piano per gli eventi avversi.

66. Stalla-Bourdillon–Knight 2017, p. 37.

67. Sul diritto alla protezione e alla circolazione dei dati, con particolare attenzione ai vantaggi derivanti dall'anonimizzazione v. Foresta 2024.

68. Richards–Hartzog 2021; Richards–Hartzog–Francis 2023.

Riferimenti bibliografici

M. Abrams (2014), *The origins of Personal Data and its implication for Governance*, in SSRN, 2014

C. Amalfitano, F. Ferri (2023), *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori,* in R. Torino, S. Zorzetto (a cura di), "La trasformazione digitale in Europa. Diritti e principi", Giappichelli, 2023

P. Barile (1987), *Democrazia e segreto*, in "Quaderni costituzionali", 1987, n. 1

L. Bolognini, C. Bistolfi (2016), *Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation*, in "Computer Law & Security Review", vol. 33, 2016, n. 2

F. Caggia (2019), *Libertà ed espressione del consenso*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

F. Calisai (2019), *I diritti dell'interessato*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

S. Calzolaio (2023), *Dalla protezione dei dati personali all'ordinamento dei dati (l'evoluzione del diritto cinese e del diritto europeo dei dati)*, in G. Di Cosimo (a cura di), "Processi democratici e tecnologie digitali", Giappichelli, 2023

S. Calzolaio (2017), *Protezione dei dati personali,* voce in "Digesto delle discipline pubblicistiche. Aggiornamento", 2017

C. Colapietro (2018), *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in "federalismi.it", 2018, n. 22

C. Colapietro, A. Iannuzzi (2017), *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro (a cura di), "Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679", Editoriale Scientifica, 2017

E. Cremona, F. Laviola, V. Pagnanelli (a cura di) (2022), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, 2022

G. D'Acquisto, M. Naldi (2017), *Big Data e privacy by Design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli, 2017

F. Di Resta (2018), *La nuova "privacy europea"*, Giappichelli, 2018

M. Elliot, K. O'Hara, C. Raab, C.M. O'Keefe, E. Mackey, C. Dibben, H. Gowans, K. Purdam, K. McCullagh (2018), *Functional Anonymisation: Personal Data and the Data Environment*, in "Computer Law & Security Review", vol. 34, 2018, n. 2

A. Esposito (2021), *Dove sono i "miei" dati? Privacy e reificazione nell'era digitale*, in "Etica & Politica/Ethics & Politics", vol. XXIII, 2021, n. 1

F. Faini (2023), *Il dato personale tra protezione giuridica e valorizzazione economica*, in "Osservatorio sulle fonti", 2023, n. 2

M. Finck, F. Pallas (2020), *They who must not be identified – distinguishing personal from non-personal data under the GDPR*, in "International Data Privacy Law", 2020, n. 1

C. Foglia (2019), *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in R. Panetta (a cura di), "Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 e al novellato d.lgs. n. 196/2003", Giuffrè, 2019

D. Foresta (2024), *Pseudonimizzazione e anonimizzazione dei dati personali contenuti nelle decisioni giudiziarie*, in "Persona e Mercato", 2024, n.1

A. Gabel, I. Schiering (2018), *Privacy Patterns for Pseudonymity*, in E. Kosta, J. Pierson, D. Slamanig (Eds.), "Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data", Springer, 2018

A. Galiano, A. Leogrande, S.F. Massari, A. Massaro (2020), *I dati non personali: la natura e il valore*, in "Rivista italiana di informatica e diritto", 2020, n. 1

C. Irti (2022), *Personal Data, Non-personal Data, Anonymised Data, Pseudonymised, De-identified Data*, in R. Senigaglia, C. Irti, A. Bernes (Eds.), "Privacy and Data Protection in software services", Springer, 2022

A. Lee Bygrave, C. Docksey, C. Kuner (2020), *The EU General Data Protection Regulation (GDPR): a commentary*, Oxford University Press, 2020

M.L. Montagnani (2019), *La libera circolazione dei dati al bivio: tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in "Mercato, concorrenza, regole", 2019, n. 2

M. Micheli, M. Ponti, M. Craglia, A. Berti Suman (2020), *Emerging models of data governance in the age of datification*, in "Big data and society", 2020, n. 2

A. Nicita (2019), *Il dato profilato nella prospettiva economica tra privacy, propertization, secrecy*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), "I dati personali nel diritto europeo", Giappichelli, 2019

P. Ohm (2010), *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in "UCLA Law Review", 2010

M. Palmirani (2019), *Prefazione*, in F. Faini, "Data society", Giuffrè, 2019

P. Passaglia (2016), *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in "Consulta online", 2016, n. 3

G.M. Riccio, G. Scorza, E. Belisario (a cura di) (2018), *GDPR e normative privacy: commentario*, Wolters Kluwer, 2018

N. Richards, W. Hartzog (2021), *A Duty of Loyalty for Privacy Law*, in "Washington University Law Review" vol. 99, 2021, n. 961

N. Richards, W. Hartzog, J. Francis (2023), *A concrete proposal for data loyalty*, in "Harvard Journal of Law & Technology", vol. 37, 2023, n. 3 Symposium

P.M. Schwartz, D.J. Solove (2011), *The PII problem: privacy and a new concept of personally identifiable information,* in "New York University Law Review", 2011

S. Stalla-Bourdillon, A. Knight (2017), *Anonymous data v. personal data – a false debate: an Eu perspective on anonymization, pseudonymization and personal data*, in "Wisconsin International Law Journal", 2017

L. Sweeney (2000), *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3, 2000

S. Torregiani (2020), *Il dato non personale alla luce del Regolamento (UE) 2018/1870: tra anonimizzazione, ownership e Data by design*, in "federalismi.it", 2020, n. 18

C.A. Trovato, C. Rauccio (2022), *L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia "dato personale-non personale"*, in "Ciberspazio e Diritto", 2022, n. 2

M. Viola De Azevedo Cunha, D. Doneda, N. Andrade (2010), *La reidentificazione dei dati anonimi e il trattamento dei dati personali per ulteriore finalità: sfide alla privacy*, in "Ciberspazio e diritto", 2010, n. 4