

I confini della nozione di dato personale nel prisma della pseudonimizzazione

Riccardo Michele Colangelo

SOMMARIO: 1. Introduzione. – 2. Considerazioni tassonomiche *de iure condito*. – 3. La nozione di pseudonimizzazione nelle Linee guida EDPB n. 1/2025. – 4. Alcune recenti pronunce giurisprudenziali in tema di pseudonimizzazione. – 4.1. La sentenza del Tribunale UE del 26 aprile 2023 (nella causa T 557/20). – 4.2. La sentenza della Corte di Giustizia dell'Unione Europea del 4 settembre 2025 (nella causa C-413/23 P). – 5. Conclusione.

1. *Introduzione*

La nozione di dato personale riveste un ruolo fondamentale nell'architettura del regolamento UE 2016/679¹ (GDPR), anche e soprattutto in relazione a quanto attiene all'ambito di applicazione materiale del medesimo.

In argomento, i soli dati qualificabili come personali costituiscono il perno dell'oggetto e della finalità del GDPR²: il regolamento generale sulla protezione dei dati è, infatti, notoriamente orientato a proteggere «i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali»³ e a favorire la «libera circolazione» dei medesimi all'interno dell'Unione⁴.

Ciò posto, il GDPR racchiude in sé una disciplina organica e *self executing* in tema di *data protection* (*rectius*: di «protezione delle persone fisiche con riguar-

¹ Si tratta, come noto, del «regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)».

² Arg. *ex art.* 1 GDPR.

³ Art. 1, par. 2 GDPR.

⁴ Art. 1, par. 3 GDPR.

do al trattamento dei dati personali»⁵), che intende non solo porre fine alla frammentazione normativa conseguente all'attuazione della direttiva 95/46/CE, nota come «direttiva-madre»⁶, ma anche perseguire significative istanze di natura economica, anche in ambito digitale⁷.

Come efficacemente riportato al considerando 7 GDPR, «è opportuno [...] che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche»: risulta pertanto fondamentale circoscrivere in modo netto l'ambito di applicazione materiale del regolamento generale sulla protezione dei dati.

A tal fine, occorre anzitutto guardare all'art. 2 GDPR, a mente del quale «il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi»⁸.

Specifici casi in cui la disciplina di cui al GDPR non può trovare applicazione sono espressamente indicati nell'articolato del medesimo regolamento⁹; d'altra parte, occorre evidenziare come al considerando 26 GDPR il legislatore europeo affermi, tra le altre cose, che «i principi di protezione dei dati non dovrebbero [...] applicarsi a 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»¹⁰.

Tale sorta di *summa divisio*¹¹ intercorrente tra dato personale e non personale riveste un ruolo fondamentale nel tracciare il confine dell'ambito di applicazione materiale del GDPR, nonostante i dubbi sollevati in dottrina – e non solo – sulla reale ed effettiva non riferibilità a una persona fisica sia del dato *ab origine*

⁵ Tale approccio è evidenziato, anche in ottica diacronica, in F. Cilia, S. Dalle Nogare, R. Pozzi, *Il principio di trasparenza*, in F. Bravo (a cura di), *Dati personali. Protezione, libera circolazione e governance – 1. Principi*, Pisa, 2023, 142 ss.

⁶ Si veda in proposito il considerando 9 GDPR. In dottrina, *ex multis*, cfr. G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in G. Resta e V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016, 117.

⁷ Cfr. considerando 6 e 7 GDPR. In particolare, è quest'ultimo a rimarcare «l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno».

⁸ Così l'art. 2, par.1, GDPR.

⁹ Si veda in proposito l'art. 2, paragrafi 2, lett. a)-d), e 3 GDPR, in relazione al quale si rimanda a quanto argomentato *infra*. Risulta opportuno evidenziare, tuttavia, come si tratti pur sempre di casi concernenti dati personali.

¹⁰ In tema di inapplicabilità della disciplina in materia di *data protection* ai dati anonimi si rimanda a R.M. Colangelo, *Ne pereant fragmenta: l'intelligenza artificiale e la complessità della Corptech governance*, in *Riv. it. inf. dir.*, 2024, 2, 637.

¹¹ O «prospettiva binaria», per utilizzare le parole di E. Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, 2, 360.

anonimo sia di quello anonimizzato successivamente, nonostante la natura irreversibile dell'anonimizzazione – a differenza della pseudonimizzazione¹².

In questo contesto, a 8 anni dalla piena applicabilità del GDPR, occorre prendere specificamente in considerazione anche la nozione di dato pseudonimizzato, nella consapevolezza che, come evidenziato al considerando 26 GDPR, «i dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile»¹³.

Nonostante il chiaro tenore letterale di tale considerando, un approccio dogmatico che ascriva sempre e comunque i dati pseudonimizzati al novero dei dati personali comporta taluni profili di criticità, rivelandosi non solo fonte di incombenze operative dettate da esigenze di *compliance*, ma anche quale potenziale ostacolo alla libera circolazione dei dati e, più in generale, all'innovazione¹⁴.

Di riflesso, la nozione di pseudonimizzazione entra in gioco anche in vari ulteriori e più recenti regolamenti, in cui il legislatore unionale ha evidenziato la rilevanza dei dati personali pseudonimizzati all'interno di discipline di dettaglio che presuppongono il riferimento a questi ultimi o, più in generale, alla misura della pseudonimizzazione¹⁵.

Occorre pertanto domandarsi quali siano gli attuali confini della nozione di pseudonimizzazione con riguardo a dati personali, evidenziando a quali condizio-

¹² *Ex multis*, cfr. ibidem, 365 e R.M. Colangelo, *op. cit.*, 637.

Significativamente, anche il legislatore unionale prende atto dei limiti di una sufficiente anonimizzazione e delle relative ricadute in tema di applicabilità del GDPR. Ciò risulta, a titolo esemplificativo, guardando al considerando 9 del regolamento UE 2018/1807, ove si afferma che – nell'attuale contesto caratterizzato anche dalla diffusione dell'utilizzo dell'intelligenza artificiale – «se i progressi tecnologici consentono di trasformare dati anonimizzati in dati personali, tali dati sono trattati come dati personali e si applica di conseguenza il regolamento (UE) 2016/679». Circa la natura irreversibile dell'anonimizzazione e reversibile della pseudonimizzazione, particolarmente interessante risulta A. Spangaro, *Anonimato della madre incapace e diritto del figlio a conoscere le proprie origini*, in *Giur. it.*, 2023, 1, 64, ove l'autrice critica la terminologia di anonimato materno, ormai «anonimato reversibile», considerando meglio attinente alla fattispecie la nozione di pseudonimizzazione.

¹³ In dottrina, in senso conforme, si veda F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 191.

¹⁴ Senza pretese di completezza, si veda M. Chierici, *Contratto di Blockchain as a Service: fondamenti teorici di una nuova prassi commerciale*, in *Contratti*, 2022, 2, 210, ove l'autore considera la pseudonimizzazione come «soluzione [...] per ovviare alle problematiche di compliance» in relazione ai trattamenti di dati personali in ambito blockchain. Si noti la differenza con il più risalente approccio di G. Finocchiaro, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 7, 1674, ove la nozione di pseudonimizzazione è ritenuta «non [...] rilevante per individuare i principi fondamentali alla base del trattamento», così come «non influenza la base giuridica del trattamento», portando l'autrice a concludere in modo netto – in tema di pseudonimizzazione – che «se le applicazioni di intelligenza artificiale utilizzano dati non anonimi si applica il Regolamento».

¹⁵ In argomento, si consideri il regolamento UE 2025/327 istitutivo dello spazio europeo dei dati sanitari Data Space (c.d. EHDS), in relazione al quale S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Nuove leggi civ. comm.*, 2025, 3, 587 ricorda che «l'accesso ai dati sanitari elettronici è garantito nel rispetto dei principi di minimizzazione dei dati e di limitazione della finalità, secondo le previsioni dell'art. 66, che distinguono le eventualità in cui i dati debbano essere anonimizzati da quelle in cui invece possano essere pseudonimizzati».

ni possa risultare corretta la sostanziale equiparazione dei dati pseudonimizzati ai dati personali, riservando attenzione anche al corollario in tema di applicabilità del regolamento generale sulla protezione dei dati.

2. *Considerazioni tassonomiche de iure condito*

Per rispondere al quesito di ricerca, risulta necessario operare una sintetica analisi preliminare dei profili tassonomici, in relazione al quadro normativo vigente in tema di *data protection*.

Guardando più nel dettaglio alle definizioni di cui al GDPR, all'articolo 4 del regolamento è possibile rinvenire le fondamentali definizioni di «dato personale» e «pseudonimizzazione».

La prima considera dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile¹⁶ («interessato»)», precisando al contempo che «si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»¹⁷.

La seconda definisce la pseudonimizzazione 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 organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile»¹⁸.

Nel GDPR – sebbene un significativo riferimento sia rinvenibile, come anticipato, nel considerando 26 – non consta alcuna espressa definizione di dato non personale¹⁹: solamente *per relationem* ed in via indiretta è possibile ricavare tale nozione, *a contrario* rispetto a quella di dato personale.

Tale approdo ermeneutico trova peraltro conferma all'interno del regolamento UE 2018/1807²⁰ ove, all'art. 3, par. 1, n. 1), vengono considerati non per-

¹⁶ Tale «collegamento funzionale» è ben evidenziato da F. Guerrieri, *sub. art. 4 GDPR*, §3, in G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2022, 43.

¹⁷ Così l'art. 4, par. 1, n. 1, GDPR.

¹⁸ Art. 4, par. 1, n. 5, GDPR.

¹⁹ In dottrina si sottolinea anche l'assenza di una nozione normativa di anonimizzazione: cfr. G. Bincoletto, *op. cit.*, 249.

²⁰ Si tratta del «regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea».

sonali «i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679».

Ciò posto, occorre considerare anche come la pseudonimizzazione, nel GDPR, più che riferirsi ad una sorta di *tertium genus* di dati²¹, assurga sovente a misura di natura tecnica²², teleologicamente orientata a perseguire una maggiore conformità del trattamento alla normativa applicabile in materia di *data protection*.

Il considerando 26 GDPR, inoltre, elenca alcuni criteri di identificabilità di una persona, statuendo che, a tal fine, «è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente»; in aggiunta, «per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione 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».

In argomento – pur trattandosi di un considerando – occorre evidenziare come tali criteri seguano l'affermazione che sostanzialmente opera un'equiparazione tra i dati pseudonimizzati e quelli personali.

In dottrina, tuttavia, sono state evidenziate alcune criticità nella formulazione di tale considerando, con particolare riguardo ai profili di indeterminazione relativi proprio ai criteri ivi enumerati: è questo il caso, a titolo esemplificativo, del riferimento necessariamente prognostico agli «sviluppi tecnologici», in assenza di paletti volti a limitare la valutazione diacronica, così come della indeterminazione circa la natura assoluta – punto di vista di «qualsiasi terzo che possa essere in grado di identificare un determinato soggetto» – o relativa – prospettiva del titolare del trattamento – per quanto attiene all'approccio da utilizzarsi «per valutare il rischio di identificazione»²³.

²¹ In senso conforme anche G. Bincoletto, *op. cit.*, 247, ove si sostiene l'assenza di «una categoria intermedia».

²² Si pensi, a titolo esemplificativo, alla pseudonimizzazione quale garanzia adeguata, da valutarsi – insieme ad altri elementi – da parte del titolare del trattamento «al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti» (così l'art. 6, par. 4, GDPR). La natura di misura tecnica risulta confermata dalle Linee guida EDPB n. 1/2025 (in relazione alle quali v. *infra*, par. 3) al n. 6, mentre al n. 23 se ne evidenziano anche profili di natura organizzativa. In dottrina, *ex multis*, cfr. C. Basunti, *Nuove prospettive di valorizzazione dei dati in dimensione collettiva: le cooperative di dati (e le reti di imprese)*, in *Contr. e impr.*, 2024, 3, 949; M. Iaselli, V. Iaselli, *Nuove tecnologie, sicurezza e protezione dei dati*, Milano, 2024, 77-78; A. Astone, *Autodeterminazione nei dati e sistemi A.I.*, in *Contr. e impr.*, 2022, 2, 434. La pseudonimizzazione e, ad onor del vero, l'anonimizzazione possono altresì essere considerate «strumenti e servizi supplementari» potenzialmente oggetto di offerta da parte dei servizi di intermediazione dei dati, ai sensi dell'art. 12 Data Governance Act: cfr. F. Bravo, *Le cooperative di dati*, in *Contr. e impr.*, 2023, 3, 778.

²³ Come efficacemente osservato da E. Pellecchia, *op. cit.*, 364-365.

3. *La nozione di pseudonimizzazione nelle Linee guida EDPB n. 1/2025*

Già il Gruppo di lavoro Articolo 29 per la protezione dei dati personali, con il Parere 4/2007 sul concetto di dati personali (WP 136), ha espressamente preso in considerazione la pseudonimizzazione – intesa quale «processo volto a mascherare l'identità» – e riconosciuto i dati pseudonimizzati, in quanto «informazioni su persone identificabili indirettamente», come dati personali²⁴: «In questo caso, pur applicandosi le norme di protezione dei dati, i rischi per le persone in relazione al trattamento delle informazioni indirettamente identificabili saranno per lo più bassi, cosicché l'applicazione di tali norme sarà a ragione più flessibile che nel caso di trattamento di informazioni su persone direttamente identificabili»²⁵.

Un apporto decisamente più significativo ed interessante è riscontrabile nelle recentissime Linee guida EDPB n. 1/2025, di cui si è chiusa alcuni mesi fa la fase di consultazione pubblica²⁶.

In attesa della versione definitiva, risulta comunque possibile formulare alcune prime considerazioni.

Escludendo quanto pertiene all'uso della pseudonimizzazione per fini di compliance al GDPR ed alle indicazioni tecniche ed operative per la sua implementazione, particolare attenzione va riservata alla parte iniziale delle Linee guida, che riguarda più direttamente la nozione di pseudonimizzazione²⁷.

L'*European Data Protection Board* – a beneficio di titolari e responsabili esterni del trattamento – ha richiamato e confermato la nozione di pseudonimizzazione riportata nel GDPR²⁸, evidenziandone i principali effetti²⁹ e ricordando, peraltro, come si tratti della prima definizione di pseudonimizzazione riscontrabile nella normativa unionale³⁰.

²⁴ Cfr. G. Bincoletto, *op. cit.*, 253.

²⁵ Gruppo di lavoro Articolo 29 per la protezione dei dati personali, Parere n. 4/2007 sul concetto di dati personali (WP 136), disponibile all'URL: <https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/1496512>.

²⁶ Le Linee guida EDPB n. 1/2025 sulla pseudonimizzazione, in consultazione pubblica dal 17 gennaio al 14 marzo 2025, risultano pubblicate, insieme ad una sintesi e a tutte le osservazioni pervenute dai diversi portatori di interessi, al seguente URL: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-012025-pseudonymisation_en. In dottrina, sulla natura complementare delle Linee guida EDPB n. 1/2025 rispetto agli approdi del Gruppo di lavoro Articolo 29, si veda C. Gallese, *Redefining Anonymization: Legal Challenges and Emerging Threats in the Era of the European Health Data Space*, in F. Casarosa, F. Gennari, A. Rossi (a cura di), *Enabling and Safeguarding Personalized Medicine. Data Science, Machine Intelligence, and Law*, Cham, 2025, 97.

²⁷ Si vedano, in particolare, i punti da 1 a 25 delle Linee guida in commento.

²⁸ Linee guida EDPB n. 1/2025, n. 3.

²⁹ Linee guida EDPB n. 1/2025, n. 4.

³⁰ Linee guida EDPB n. 1/2025, n. 1.

Anche in queste Linee guida è possibile rinvenire una conferma, ad onore del vero maggiormente articolata, dell'applicabilità della normativa in materia di *data protection* ai dati pseudonimizzati: «I dati pseudonimizzati, che potrebbero essere attribuiti a una persona fisica tramite l'uso di informazioni aggiuntive, devono essere considerati informazioni riguardanti una persona fisica identificabile e, pertanto, dati personali. Questa affermazione rimane valida anche se i dati pseudonimizzati e le informazioni aggiuntive non si trovano nelle mani della stessa persona. Se i dati pseudonimizzati e le informazioni aggiuntive possono essere combinati, tenendo conto dei mezzi ragionevolmente utilizzabili dal titolare del trattamento o da un'altra persona, allora i dati pseudonimizzati sono personali. Anche se tutte le informazioni aggiuntive detenute dal titolare che effettua la pseudonimizzazione sono state cancellate, i dati pseudonimizzati diventano anonimi solo se sono soddisfatte le condizioni per l'anonimato»³¹.

Infatti, a carico dei titolari del trattamento che vogliono pseudonimizzare dati personali, le Linee guida individuano una triade di operazioni da svolgere, incentrate, tra l'altro, sulla necessaria attenzione da riservarsi a tutte le parti dei dati personali, non solo agli pseudonimi³², e sulla consapevolezza dell'insufficienza della trasformazione dei dati, che deve necessariamente essere corroborata da misure tecniche e organizzative aggiuntive che «limitano l'accesso alle informazioni aggiuntive conservate (ad esempio chiavi o tabelle di pseudonimi) e controllano il flusso dei dati pseudonimizzati» e, in quanto tali, sono finalizzate ad evitare l'abbinamento tra dato pseudonimizzato e persona fisica³³.

Le Linee guida, oltre ad analizzare le nozioni di attribuzione³⁴ e informazioni aggiuntive³⁵, introducono il nuovo concetto di dominio di pseudonimizzazione («*pseudonymisation domain*»)³⁶, il quale «può [...] coincidere con un insieme di destinatari legittimi previsti dei dati pseudonimizzati»³⁷, ma può anche essere esteso da parte del «titolare che effettua la pseudonimizzazione» a soggetti diffe-

³¹ Linee guida EDPB n. 1/2025, n.22, traduzione italiana dell'autore. In merito all'anonimizzazione dei dati, si vedano il parere del Gruppo di lavoro articolo 29 n. 5/2014 sulle tecniche di anonimizzazione (WP216) e lo standard ISO/IEC 27559:2022 (Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework).

³² Ciò nella consapevolezza che l'ampiezza della nozione di pseudonimizzazione riportata nel GDPR risulta maggiore rispetto a quanto sia percepita nella prassi dei trattamenti di dati personali. Si vedano in proposito le Linee guida, n. 7, ove si afferma che: «*The legal definition takes a more comprehensive view of the effect of pseudonymisation. It shall no longer be possible to attribute the personal data to a specific data subject without the use of additional information. This requires a look at all parts of the personal data, not only the pseudonyms*».

³³ Così le Linee guida EDPB n. 1/2025, n. 9, traduzione italiana dell'autore. Si vedano, in proposito, anche i nn. 5, 7 e 8.

³⁴ Ivi, n. 17.

³⁵ Ivi, n. 19.

³⁶ Cfr. ivi, n. 10 e, più nel dettaglio, nn. 35-43.

³⁷ Ivi, n. 36, traduzione dell'autore.

renti «ma che potrebbero comunque tentare di accedervi [...] al fine di mitigare gli effetti negativi di un accesso non autorizzato da parte di tali soggetti»³⁸.

Nelle Linee guida in commento emerge, pertanto, una nozione di pseudonimizzazione in funzione del destinatario legittimo (e non).

4. *Alcune recenti pronunce giurisprudenziali in tema di pseudonimizzazione*

Gli interessanti elementi emersi da una lettura non superficiale del considerando 26 GDPR, dall'elaborazione dottrinale e dalla disamina delle Linee guida EDPB n. 1/2025 possono essere arricchiti da ulteriori spunti di natura giurisprudenziale a livello eurounitario.

Nello specifico, in questa sede vengono sinteticamente prese in considerazione due pronunce, entrambe concernenti l'interpretazione di norme del regolamento UE 2018/1725, «sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE».

Nonostante si tratti di un regolamento diverso dal GDPR, è necessario evidenziare in via preliminare la sostanziale sovrapponibilità delle definizioni in questione, peraltro consacrata dall'art. 2, par. 3, GDPR che, in relazione all'ambito di applicazione materiale del regolamento, sancisce che «il regolamento (CE) n. 45/2001» – successivamente abrogato appunto dal regolamento UE 2018/1725 – «e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98».

4.1. *La sentenza del Tribunale UE del 26 aprile 2023 (nella causa T557/20)*

La prima sentenza rilevante è stata pronunciata dal Tribunale eurounitario, Ottava sezione ampliata, il 26 aprile 2023, nella causa T-557/20³⁹: in accoglimento del primo motivo di ricorso, è stata annullata la decisione rivista⁴⁰ del Garante europeo della protezione dei dati (GEPD), che era stata adottata in data 24 novembre 2020 contro il Comitato di risoluzione unico (CRU).

³⁸ Ivi, n. 37, traduzione dell'autore.

³⁹ Trib. UE, 26 aprile 2023, causa T-557/20.

⁴⁰ In esito al riesame, su richiesta del Comitato di risoluzione unico, di una precedente decisione del GEPD, del 24 giugno 2020.

Nel contesto di un programma di risoluzione per il Banco Popular Español, SA, il CRU aveva avviato il procedimento relativo al diritto di essere ascoltati, invitando azionisti e creditori ad inviare osservazioni, successivamente trasmesse dallo stesso Comitato a Deloitte, società che, come esplicitato al punto 24 della sentenza in commento, «non aveva e non ha tuttora accesso alla banca dati contenente i dati raccolti durante la fase di iscrizione».

Nel raccogliere tali dati, il CRU aveva ommesso di indicare, nell'informativa resa agli interessati, che le osservazioni, una volta pseudonimizzate, sarebbero state trasmesse a Deloitte: ciò in violazione – secondo quanto statuito dal GEPD – dell'obbligo informativo previsto *ex art.* 15, par. 1, lett. d), regolamento UE 2018/1725.

Con specifico riguardo al primo dei due motivi a sostegno del ricorso, il CRU ha lamentato che il «GEPD ha violato l'articolo 3, punto 1, del regolamento 2018/1725 ritenendo, nella decisione rivista, che le informazioni trasmesse a Deloitte costituissero dati personali dei reclamanti» (punto 57).

Il Tribunale, richiamando la sentenza del 19 ottobre 2016, Breyer (C582/14, EU:C:2016:779)⁴¹, ha evidenziato che «per stabilire se le informazioni trasmesse a Deloitte costituissero dati personali, occorre porsi dal punto di vista di quest'ultima per determinare se le informazioni che le sono state trasmesse si riferiscano a «persone identificabili»⁴².

È proprio sul punto di vista che si fonda la censura delle motivazioni del provvedimento impugnato, in quanto, secondo il Tribunale, «il GEPD si è limitato ad esaminare la possibilità di reidentificare gli autori delle osservazioni dal punto di vista del CRU e non di Deloitte»⁴³, non ritenendo necessaria alcuna verifica degli elementi che, in concreto, avrebbero potuto condurre (o meno) alla potenziale reidentificazione degli interessati da parte della società⁴⁴.

Sulla base di tale argomentazione, è stato affermato che, nel caso di specie, «il GEPD non poteva concludere che le informazioni trasmesse a Deloitte costituissero informazioni concernenti una «persona fisica identificabile» ai sensi dell'articolo 3, punto 1, del regolamento 2018/1725»⁴⁵.

In relazione a tale pronuncia, la dottrina ha riconosciuto un cambiamento di rotta a livello giurisprudenziale, caratterizzato da un allontanamento rispetto all'interpretazione piuttosto letterale delle norme che, nel GDPR, regolano l'isti-

⁴¹ CGUE, 19 ottobre 2016, causa C-582/14 circa la natura personale o meno degli indirizzi IP dinamici.

⁴² Trib. UE, 26 aprile 2023, causa T-557/20, n. 97.

⁴³ Ivi, n. 103.

⁴⁴ Ivi, n. 101.

⁴⁵ Ivi, n. 105.

tuto, «*towards a personalized concept of anonymization and pseudonymization, in contrast with Recital 26 of the GDPR and the previous Patrick Breyer case*»⁴⁶.

È stata pertanto individuata tale tensione verso una nozione personalizzata di pseudonimizzazione, che tiene conto della prospettiva di ciascuna parte coinvolta nel trattamento e del relativo livello di controllo dei dati, ed in particolare dei destinatari dei dati e della loro effettiva capacità di reidentificazione⁴⁷, pur nella consapevolezza che ancorare la natura personale o meno di un dato al contesto dello specifico trattamento, senza considerarla intrinsecamente correlata al dato stesso, non coincida del tutto con la *ratio* sottesa alle norme in materia di *data protection*⁴⁸.

4.2. *La sentenza della Corte di Giustizia dell'Unione Europea del 4 settembre 2025 (nella causa C-413/23 P)*

Simili considerazioni possono effettuarsi anche in relazione alla recentissima sentenza pronunciata dalla Corte di Giustizia dell'Unione Europea, Prima Sezione, in data 4 settembre 2025⁴⁹.

In argomento, è possibile affermare che tale arresto giurisprudenziale risulta ancor più rilevante non solo in virtù del mero fattore temporale, ma anche – e soprattutto – in quanto nasce dalla impugnazione, da parte del GEPD, proprio della sentenza del Tribunale dell'Unione europea del 26 aprile 2023.

La CGUE ha annullato la sentenza del Tribunale dell'Unione europea del 26 aprile 2023 in accoglimento del primo motivo di ricorso, rinviando per il resto la causa T 557/20 al Tribunale dell'Unione europea, in quanto «lo stato degli atti non consente di statuire sulla controversia per quanto riguarda il secondo motivo di ricorso[, concernente la violazione dell'articolo 4, paragrafo 2, e dell'articolo 26, paragrafo 1, del regolamento 2018/1725,] dal momento che tale motivo implica valutazioni di fatto che non sono state operate dal Tribunale»⁵⁰.

⁴⁶ C. Gallese, *op. cit.*, 97.

⁴⁷ In senso conforme, si veda anche S. Franca, *Il regime del trattamento di dati personali: persistenti incertezze e nuovi capisaldi*, in *Giorn. dir. amm.*, 2024, 3, 357, costituente nota a CGUE, 5 dicembre 2023, causa C-683/21.

⁴⁸ Cfr. C. Gallese, *op. cit.*, 98, ove peraltro si afferma quanto segue: «*If the original context determines whether data qualifies as “personal”, the third party with whom the dataset is shared may argue that the GDPR does not apply because the data was shared as “non-personal”. This creates a loophole for re-identification and potential privacy breaches. By contrast, qualifying the “personal” aspect of the data as inherently tied to the data itself, rather than contingent on the context of its processing or the entities involved, better aligns with the GDPR’s intent to provide consistent protection.*».

⁴⁹ CGUE, 4 settembre 2025, causa C-413/23 P.

⁵⁰ Ivi, n. 121.

Per quanto attiene al primo motivo di impugnazione – vertente, in estrema sintesi, sulla violazione dell’articolo 3, punti 1 e 6, del regolamento 2018/1725 e, quindi, sulle nozioni di dato personale e pseudonimizzazione – la Corte ha preliminarmente evidenziato una sovrapposibilità in tali definizioni, come contenute nel regolamento *de quo*, nel GDPR e nella stessa direttiva madre, ritenendo pertanto doveroso «garantire un’applicazione uniforme e coerente del diritto dell’Unione» mediante «un’interpretazione identica dell’articolo 3, punto 1, del regolamento 2018/1725, dell’articolo 4, punto 1, del RGPD e dell’articolo 2, lettera a), della direttiva 95/46»⁵¹.

L’annullamento della sentenza del Tribunale è stato disposto – come efficacemente sintetizzato al punto 111 – sulla base del presupposto che, «ai fini dell’applicazione dell’obbligo di informazione previsto all’articolo 15, paragrafo 1, lettera d), del regolamento 2018/1725, l’identificabilità dell’interessato debba essere valutata al momento della raccolta dei dati e dal punto di vista del titolare del trattamento», in relazione al quale è indubbio che i dati pseudonimizzati rivestano carattere personale⁵².

Per quanto maggiormente interessa in questa sede, occorre sottolineare come tale principio non osti in alcun modo alla emergente nozione relativa di pseudonimizzazione.

La Corte, infatti, dopo aver premesso che «i dati pseudonimizzati [...] non sono menzionati nella definizione legale della nozione di “dati personali”»⁵³, e che «la pseudonimizzazione non costituisce quindi un elemento della definizione dei «dati personali», ma si riferisce all’attuazione di misure tecniche e organizzative dirette a ridurre il rischio di mettere in correlazione un insieme di dati con l’identità degli interessati»⁵⁴, ha confermato che – in presenza di effettive ed idonee misure tecniche ed organizzative – «la pseudonimizzazione può incidere sul carattere personale di tali dati»⁵⁵ segnatamente dal punto di vista del destinatario (nel caso di specie: Deloitte), per il quale i dati personali oggetto di comunicazione non presentano carattere personale⁵⁶.

⁵¹ Ivi, n. 52.

⁵² Come evidenziato ivi, al n. 100, «secondo la giurisprudenza derivante segnatamente dalla sentenza del 19 ottobre 2016, Breyer (C 582/14, EU:C:2016:779) [...] la prospettiva pertinente per valutare l’identificabilità dell’interessato dipende essenzialmente dalle circostanze che caratterizzano il trattamento dei dati in ciascun caso particolare». La Corte afferma espressamente di porsi in continuità con tale approccio giurisprudenziale, individuando la prospettiva del titolare del trattamento come la più idonea ai fini del rispetto del principio di trasparenza nei confronti degli interessati, con particolare riguardo a quanto concerne l’indicazione dei destinatari dei dati.

⁵³ CGUE, 4 settembre 2025, causa C-413/23 P, n. 71.

⁵⁴ Ivi, n. 72.

⁵⁵ Ivi, n. 75.

⁵⁶ Ivi, n. 77.

Secondo la Corte, le «precisazioni relative alla valutazione del carattere identificabile o meno dell'interessato» di cui al considerando 16 del regolamento 2018/1725, il cui tenore letterale risulta sostanzialmente sovrapponibile al considerando 26 GDPR, «sarebbero private di qualsiasi effetto utile se dati pseudonimizzati dovessero essere considerati come costituenti, in ogni caso e per qualsiasi persona, dati personali ai fini dell'applicazione del regolamento 2018/1725»⁵⁷.

In argomento, ancor più efficacemente, al punto 86, la Corte ha evidenziato la necessità di una valutazione caso per caso: «contrariamente a quanto sostiene il GEPD, non si deve ritenere che i dati pseudonimizzati costituiscano, in ogni caso e per qualsiasi persona, dati personali ai fini dell'applicazione del regolamento 2018/1725, in quanto la pseudonimizzazione può, a seconda delle circostanze del caso di specie, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato in modo tale che, per esse, quest'ultimo non sia o non sia più identificabile».

La nozione di dato personale, infatti, «non è illimitata, dal momento che la disposizione citata richiede segnatamente che l'interessato sia identificato o identificabile», nonostante risulti chiaro «l'obiettivo del legislatore dell'Unione di attribuire un significato ampio alla nozione» medesima⁵⁸.

5. *Conclusioni*

L'analisi condotta ha permesso di evidenziare come non sia (più) possibile considerare *sic et simpliciter* i dati pseudonimizzati come dati personali: infatti, se rimangono tali per il soggetto che effettua la pseudonimizzazione, non è possibile individuare una corrispondenza necessaria in tutti quei casi in cui un soggetto non sia materialmente nelle condizioni di ricostruirne l'attribuzione a specifiche persone fisiche, servendosi di informazioni supplementari.

In estrema sintesi, lo stesso *dataset* pseudonimizzato potrebbe, da prospettive diverse – come nella dialettica dei flussi di dati tra titolari autonomi o tra titolare e responsabile – assumere una diversa qualificazione giuridica, in quanto composto, per l'uno, da dati personali e, per l'altro, da dati che, sebbene non anonimizzati, risultano in concreto non riconducibili a specifiche persone fisiche, le quali permangono non identificabili, seppur indirettamente, in modo agevole e legittimo.

Si assiste, pertanto, alla netta emersione di una nozione relativa di pseudonimizzazione, similmente a quanto riscontrabile circa quella di anonimizzazione, in relazione alla quale sia il parere del Gruppo di lavoro Articolo 29 n. 5/2014 sulle

⁵⁷ Ivi, n. 80.

⁵⁸ Ivi, n. 88.

tecniche di anonimizzazione (WP216) sia lo standard ISO/IEC 27559:2022 evidenziano la necessità di una valutazione (e gestione) del rischio di reidentificazione in funzione dello specifico destinatario dei dati, al fine di perseguire una sufficiente anonimizzazione⁵⁹.

Inoltre, tale natura essenzialmente bifronte dei dati pseudonimizzati reca con sé alcune rilevanti ricadute per quanto concerne l'applicabilità della normativa in materia di *data protection*: esse meritano ulteriori approfondimenti, anche in relazione a potenziali esiti non del tutto condivisibili, che rischiano, di fatto, di imporre adempimenti eccessivi a carico di chi comunica dati personali – previa adeguata pseudonimizzazione degli stessi – a destinatari oggettivamente privi dei mezzi e delle informazioni necessarie per compiere il procedimento inverso.

⁵⁹ R.M. Colangelo, *op. cit.*, 638.

I confini della nozione di dato personale nel prisma della pseudonimizzazione

Il paper intende indagare, nel contesto della tassonomia propria del GDPR, gli attuali confini della nozione di pseudonimizzazione, anche in un'ottica diacronica, al fine di porre in luce a quali condizioni sia corretta la sostanziale equiparazione dei dati pseudonimizzati ai dati personali.

Tale analisi, pertanto, contribuisce ad una migliore delimitazione del confine tra dati personali e dati non personali, foriera di rilevanti implicazioni in tema di applicabilità del GDPR.

L'illustrazione e l'interpretazione del dettato normativo risultano corroborate dal riferimento a recenti linee guida dell'European Data Protection Board (EDPB) e ad alcuni arresti giurisprudenziali eurounitari particolarmente recenti e rilevanti, che evidenziano la natura sempre più dinamica della nozione di pseudonimizzazione, la quale richiede valutazioni caso per caso.

The Boundaries of the Notion of Personal Data through the Prism of Pseudonymisation

This paper aims to examine, within the taxonomy established by the GDPR, the current boundaries of the notion of pseudonymisation, including from a diachronic perspective, in order to shed light on the conditions under which the assimilation of pseudonymised data to personal data is justified. The analysis therefore contributes to a more precise delineation of the boundary between personal and non-personal data, a distinction that carries significant implications for the material scope of the GDPR. The exposition and interpretation of the relevant legal framework are supported by reference to recently issued guidelines of the European Data Protection Board (EDPB) and significant rulings of the EU courts, which underscore the increasingly dynamic nature of the notion of pseudonymisation and the resulting need for case-by-case assessments.