L'uso degli Pseudonimi e gli obblighi informativi del titolare del trattamento: la Corte di Giustizia chiarisce i limiti dell'art. 3 reg. (UE) 2018/1725

di Diletta Sagliocco

Title: The use of Pseudonyms and the data controller's information obligations: the Court of Justice clarifies the limits of article 3 of Regulation (EU) 2018/1725

Keywords: Data protection; Pseudonymisation; Personal data

1. - Nella sentenza in commento la Corte di Giustizia dell'Unione europea è stata chiamata a pronunciarsi sulla nozione di "dato personale", con specifico riguardo alla qualificazione e al valore giuridico dei dati *pseudonimizzati*, nonché agli obblighi informativi gravanti sul titolare del trattamento ai sensi del Regolamento (UE) 2018/1725. La questione interpretativa deferita alla Corte di Giustizia verte sul corretto inquadramento giuridico dei dati *pseudonimizzati* e sugli obblighi informativi gravanti sul titolare del trattamento, ai sensi del Regolamento (UE) 2018/1725. Tale strumento normativo, volto a disciplinare la protezione dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione europea, riconosce all'interessato un diritto specifico a conoscere i soggetti ai quali le proprie informazioni vengono comunicate (art. 15, par. 1, lettera d). Si tratta di una garanzia che concretizza ed attua il principio di trasparenza — pilastro essenziale dell'ordinamento europeo in materia di protezione dei dati — rafforzando la tutela del diritto all'informazione del soggetto interessato. In coerenza con quanto già previsto dal Regolamento (UE) 2016/679 (GDPR), consolidatosi come il principale strumento giuridico dell'Unione in materia di protezione dei dati (Z. He, *From privacy-enhancing to health data utilisation: The traces of Anonymisation and Pseudonymisation in EU data protection law*, in 2 ***DISO*** 6 (2023)), il Regolamento del 2018 rafforza le garanzie a favore delle persone fisiche, assicurando loro la piena comprensione, in forma chiara e accessibile, delle modalità di raccolta, utilizzo, consultazione e ulteriore trattamento dei propri dati, nonché della portata e delle finalità delle operazioni compiute. Il nuovo quadro normativo, estendendo la protezione dei dati anche al livello istituzionale dell'Unione, assicura la piena coerenza con il sistema di tutele già previsto per imprese, enti, professionisti e amministrazioni nazionali dal GDPR, ampliando così lo spettro di operatività del diritto fondamentale alla protezione dei dati personali.

La controversia origina da una procedura di risoluzione bancaria promossa dal Comitato di risoluzione unico (SRB), il quale aveva provveduto alla trasmissione di dati *pseudonimizzati* concernenti azionisti e creditori a consulenti esterni, in particolare alla società di revisione Deloitte, nell'ambito di una procedura di

DPCE online
ISSN: 2037-6677

indennizzo. Il SRB aveva ritenuto che tale pseudonimizzazione esentasse il trattamento dagli obblighi informativi previsti dal Regolamento sopra citato. A seguito di reclami presentati da più soggetti interessati, il GEPD (Garante europeo della protezione dei dati) rilevava la violazione degli obblighi di trasparenza da parte del SRB, intimandone il tempestivo adeguamento alla normativa comunitaria vigente.

Con la presente impugnazione, il GEPD domanda l'annullamento della sentenza del Tribunale dell'Unione europea del 26 aprile 2023 (Cfr. Trib. UE, sent. 26.4.2023, T-557/20, *Single Resolution Board*), con cui quest'ultimo ha annullato la decisione di revisione adottata dal GEPD il 24 novembre 2020 (Cfr. GEPD, Dec. di revisione SRB, 24-11- 2020, modif. Dec. 24-06-2020). Tale revisione era stata disposta a seguito della richiesta di riesame formulata dal SRB avverso la precedente decisione del GEPD del 24 giugno 2020, concernente cinque reclami presentati da più soggetti.

La CGUE, ribaltando la decisione di primo grado del Tribunale dell'Unione Europea (T-557/20), ha con fermezza escluso che i dati *pseudonimizzati*, sebbene trasmessi a terzi, possano sottrarsi all'ambito di applicazione del Regolamento del 2018. Si è affermato, infatti, che il criterio determinante per la qualificazione di "dato personale" non risiede nella mera tecnica di trattamento adottata o nella forma con cui i dati sono presentati, bensì nella concreta e attuale possibilità di identificazione dell'interessato (cfr. Corte giust., sent. 19 - 10 - 2016, C-582/14, *Patrick Breyer*). In tale prospettiva, è stato precisato che la pseudonimizzazione non si identifica con l'anonimizzazione, poiché, diversamente dai dati anonimi, quelli *pseudonimizzati* restano assoggettati alla disciplina del GDPR, in quanto il rischio di re-identificazione permane più elevato. Solo i dati effettivamente anonimizzati risultano idonei a sottrarsi in modo definitivo all'ambito di applicazione della normativa sulla protezione dei dati personali (P. Voigt, A. Von dem Bussche, *The eu general data protection regulation (gdpr). A practical guide*, 1st ed., Cham, 2017, 15 ss.). Di conseguenza, permane la potenziale ri-identificazione mediante informazioni supplementari, se quest'ultime non 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» (cfr. art. 4, par. 5 GDPR). L'identificabilità dipende dal soggetto e va valutata al momento della raccolta e dal punto di vista del titolare, non solo del destinatario a cui i dati vengono in seguito trasmessi. Tale principio riflette l'esigenza di una valutazione dinamica e contestuale, che consideri tutte le informazioni effettivamente disponibili al titolare per determinare se un dato possa effettivamente essere ricondotto a una persona fisica identificabile. Ne discende che il dato *pseudonimizzato* conserva a pieno titolo la qualifica di *"dato personale"*, imponendo, senza eccezioni, al titolare del trattamento l'osservanza integrale degli obblighi previsti dal Regolamento, con particolare riguardo a quelli informativi sanciti dall'art. 15, sopra menzionato. L'identificabilità di un dato *pseudonimizzato* dipende, dunque, dalla relazione tra titolare e destinatario, dai mezzi effettivamente disponibili e dalla probabilità reale di re-identificazione (M. Gorga, *Profili giuridici nella protezione dei dati nella ricerca scientifica in ambito accademico*, Milano, 2025, 15 ss.).

Ulteriormente, la pronuncia evidenzia che la comunicazione di dati *pseudonimizzati* a terzi costituisce una forma di comunicazione che, in ossequio ai principi di lealtà e correttezza del trattamento (artt. 5 e 6 Regolamento 2018/1725), determina un obbligo specifico di informazione nei confronti degli interessati (art. 15). Tale obbligo rappresenta uno strumento essenziale volto a garantire il pieno esercizio dei diritti attribuiti agli interessati, principi ancorati nelle disposizioni della Carta dei diritti fondamentali dell'Unione europea, in particolare all'art. 8, par.

2 (M. Brewczyńska, *Between legitimacy and lawfulness: In search of rationality and consistency in EU data protection*, in 9 *EDPL* 115 (2023)).

La pronuncia si inserisce nel solco interpretativo già tracciato dalla Corte in materia di protezione dei dati personali, consolidando il principio per cui la tecnica della pseudonimizzazione, pur essendo una misura di sicurezza idonea a mitigare i rischi, non esclude la qualificazione giuridica di dato personale né esonera il titolare del trattamento dagli obblighi informativi e di protezione (cfr. Corte giust., *Breyer*).

2. – La *pseudonimizzazione* è un concetto dinamico, strettamente connesso al progresso tecnologico (E. Podda, M. Palmirani, *Inferring the meaning of non-personal, anonymized, and anonymous data*, in V. Rodríguez-Doncel e al. (Eds.) *AI Approaches to the Complexity of Legal Systems XI-XII*, Cham, 2018, 269-282). La questione interessa le normative nazionali in materia di protezione dei dati personali, con particolare riguardo al Regolamento del 2018 e alle specifiche declinazioni operanti nei principali ordinamenti membri, quali quello spagnolo, italiano e francese. Solo alla luce di tale quadro può comprendersi appieno la portata e l'innovatività della recente sentenza, nonché le conseguenze applicative in ordine agli obblighi del titolare del trattamento e alle tutele riconosciute agli interessati. La normativa spagnola riconosce la tutela delle persone fisiche in relazione al trattamento dei dati personali quale diritto fondamentale, già all'interno della Carta costituzionale (art. 18, par. 4). Il legislatore costituzionale iberico si è posto come anticipatore nel panorama europeo, elevando la protezione dei dati personali a presidio essenziale della dignità umana e dell'autodeterminazione informativa (E. B. Cuadrada, *La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad*, in *Rev. Inter. Der. Pol.*, 2007, n. 5, 83). Attraverso la *Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales* (LOPDGDD) recepisce e sviluppa integralmente il Regolamento GDPR (all'art. 1 comma a) e la Direttiva (UE) 2016/680 concernente la tutela delle persone fisiche rispetto al trattamento dei dati personali da parte delle autorità competenti in materia penale, assicurando al contempo la libera circolazione di tali dati nell'Unione (M. N. Martínez Rodríguez, *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, in *Ars Iuris Salmanticensis*, 2019, 233). La LOPDGDD, di portata sistematica e innovatrice, ha armonizzato l'ordinamento spagnolo con i principi europei in materia di protezione dei dati, consolidando un modello coerente e trasparente di tutela. Tale intervento si innesta sul precedente tracciato della *Ley Orgánica 5/1992*, che aveva introdotto per la prima volta una disciplina organica della materia e istituito *l'Agencia Española de Protección de Datos* (AEPD), autorità indipendente incaricata di vigilare sull'applicazione della normativa e di garantire l'effettiva protezione dei diritti degli interessati (S. Morales-Ferrer, *La agencia española de protección De datos: un estudio breve sobre su Naturaleza jurídica, su régimen jurídico y su estructura tanto estatal como Autonómica*, in *Novum Jus*, 2020, n. 2, 174). L'AEPD in diversi modi, attraverso guide e risoluzioni, ha evidenziato come la pseudonimizzazione sia una tecnica, per cui i dati così trattati restano soggetti alla disciplina del GDPR e della LOPDGDD (AEDP, *Guía para la correcta elaboración de un modelo de hoja de información al paciente y consentimiento informado (HIP(CI))*, N/REF: 040931/2019; AEDP, *Resolución del procedimiento sancionador EXP202409872 c Dirección General de la Guardia Civil por vulneración del artículo 32 del RGPD*, Madrid, 2025). Tale posizione trova piena consonanza con l'impostazione seguita dalla Corte di giustizia nella sentenza in esame, in accorso con l'orientamento della AEPD e della legislazione nazionale, secondo cui tali dati mantenevano la natura personale, poiché l'identificazione non era esclusa, ma solo sospesa temporaneamente, in quanto il SRB, pur applicando misure di

DPCE online
ISSN: 2037-6677

pseudonimizzazione, deteneva le chiavi di corrispondenza che consentivano la re-identificazione dei soggetti coinvolti. L'ordinamento spagnolo manifesta così una concezione rigorosa circa l'anonimato, orientata a garantire un elevato livello di protezione dei dati personali, in osservanza degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. In tale contesto, la pseudonimizzazione in Spagna non costituisce una deroga al regime di protezione, bensì una misura integrativa espressiva del principio di responsabilizzazione proattiva (*accountability*), secondo cui il titolare del trattamento deve non solo essere in grado di rispettare tutti i principi del trattamento dei dati, ma deve «essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento» (considerando 74 GDPR; J. L. Lopes da Mota, G. Pérez Souto, *Publicación on-line de las decisiones judiciales en Europa, derechos fundamentales y protección de datos a la luz del RGPD:¿ misión cumplida?*, in *Rev. Gen. Der. Eur.*, 2019, n. 49, 38). Questa interpretazione trova adeguato riscontro anche nell'ordinamento italiano, dove il Codice in materia di protezione dei dati personali (d.lgs. 196/2003, modificato dal d.lgs. 101/2018), recepisce il GDPR. La definizione di pseudonimizzazione viene fornita dal d.lgs. 51/2018 adottato in esecuzione della delega contenuta nell'art 11 della L. 167/2017 e identificato come un decreto di "attuazione" della Direttiva UE 2016/680, finalizzato a recepirne il contenuto nell'ordinamento italiano (R. Bifulco et al., *Protezione dei dati personali in Italia tra GDPR e codice novellato-e-Book*, Torino, 2021, 9). All'art. 2, comma 1, lettera d si legge che per *pseudonimizzazione*, s' intende il trattamento dei dati che impedisce l'identificazione diretta di una persona senza informazioni aggiuntive, le quali devono essere conservate separatamente e protette da misure tecniche e organizzative adeguate. Tale formulazione, conforme al tenore letterale dell'art. 4, punto 5, del GDPR, riflette il principio cardine ribadito dalla CGUE nella sentenza in commento. In perfetta consonanza con tale approccio ermeneutico, il legislatore italiano ha ulteriormente precisato l'ambito di applicazione di tali principi in materia settoriale. Il D. L. 19/2024, poi, convertito in legge nel maggio 2024 con la L. 56/2024, introduce disposizioni per il trattamento dei dati personali sanitari, *pseudonimizzati*, in conformità con il PNRR (art. 2 sexies comma 1 bis e ter). Conformemente a quanto fatto dalla CGUE nella pronuncia in esame, anche il Garante italiano per la protezione dei dati personali ha esaminato un ampio ventaglio di reclami, segnalazioni e richieste di parere concernenti questioni attinenti al trattamento di dati personali. Il Garante ha più volte ribadito che la pseudonimizzazione costituisce una misura di sicurezza interna al trattamento e non una modalità idonea a escludere l'applicazione della disciplina di tutela dei dati personali. In un caso in particolare, il Garante ha irrogato una sanzione amministrativa pecuniaria a carico di un istituto scolastico responsabile della pubblicazione di numerose determinazioni dirigenziali, sul proprio sito istituzionale, relative alle assenze dal servizio del personale docente e di altro personale scolastico (Garante per la protezione dei dati personali, provv. 24-01-2024, n. 35, doc. par. 13.3, www.garanteprivacy.it). Nel corso dell'istruttoria è emerso che l'istituto aveva proceduto alla raccolta e alla conservazione dei dati personali degli alunni per lo svolgimento di una iniziativa di ricerca scientifica, operando per conto di un'università senza essere stato formalmente designato ai sensi dell'art. 28 del GDPR e senza disporre di una idonea base giuridica a legittimare il ruolo concretamente assunto di autonomo titolare del trattamento, con conseguente violazione degli artt. 6 e 9 del medesimo Regolamento. Rilevando che la mera pseudonimizzazione dei nominativi non impediva la re-identificazione degli interessati, tale pronuncia, nel ribadire che i dati *pseudonimizzati* restano pienamente soggetti alle disposizioni del GDPR, richiama in modo quasi testuale i principi affermati dalla Corte, secondo cui il carattere personale del dato non si estingue per effetto della pseudonimizzazione, trattandosi di una mera misura di protezione interna che si limita a ridurre la correlabilità di un insieme di dati

all'identità originaria di un interessato e rappresenta pertanto una misura che il titolare del trattamento è tenuto ad implementare e non di una tecnica di anonimizzazione in senso proprio (Cfr. Garante per la protezione dei dati personali, provv. 13-11-2024, n.674, doc. par. 2, www.garanteprivacy.it).

Un'analoga evoluzione si riscontra nel contesto francese, dove la *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* – tra le prime al mondo in materia di protezione dei dati personali – è stata profondamente riformata dalla *Loi n° 2018-493 du 20 juin 2018* e dal *Décret n° 2019-536 du 29 mai 2019*, in ossequio all'obbligo di adeguamento al GDPR, conformandola ai principi e alle disposizioni sanciti dal nuovo quadro normativo europeo (O. Tambou, *France: the french approach to the gdpr implementation*, in 4 *Eur. Data Prot. L. Rev.* 88 (2018)). In Francia, il diritto alla riservatezza (*vie privée*) trova protezione nell'art. 9 del *Code Civil* che protegge la vita privata («chacun a droit au respect de sa vie privée»). Il problema della pseudonimizzazione è emerso in seguito alla diffusione del rapporto redatto dalla cosiddetta commissione *Cadiet* istituita con l'obiettivo di approfondire – e quindi solo a posteriori – le implicazioni derivanti dalla riforma (L. Cadiet, *Rapport sur l'open data des décisions de justice*, Ministère de la Justice, 2017). Parallelamente l'Autorità francese per la protezione dei dati personali, la *Commission Nationale de l'Informatique et des Libertés* (CNIL), istituita dalla legge del 6 gennaio 1978, ha da sempre pubblicato un vasto ventaglio di documenti, in ambito nazionale ed internazionale, volti a fornire orientamenti interpretativi e linee guida pratiche rispetto all'applicazione delle disposizioni legislative nazionali ed europee, stabilendo altresì procedure corrette e conformi da adottare (P. Guarda, G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Milano, 2023, 112). Tra questi si segnalano la deliberazione del 5 settembre 2024 in cui la CNIL, perfettamente in linea con la *ratio* della sentenza in oggetto, ha sanzionato un titolare del trattamento che aveva ritenuto erroneamente di poter considerare come anonimizzati dati sanitari sottoposti unicamente a pseudonimizzazione (CNIL, *Délibération n° SAN-2024-013 du 5 septembre 2024*, www.legifrance.gouv.fr); e il parere tecnico, fornito dall'organismo europeo WP29 cui la CNIL ha partecipato come membro, nel quale è stato sancito che dati sottoposti a pseudonimizzazione non possono essere equiparati a quelli anonimizzati, in quanto non escludendo in modo definitivo la riconducibilità del dato alla persona fisica interessata, perdurano nel rientrare nell'alveo di applicazione della disciplina giuridica in materia di protezione dei dati personali (Groupe de travail «Article 29» sur la protection des données, *Avis 05/2014 sur les techniques d'anonymisation*, 0829/14/FR, WP216, Bruxelles, 10 avril 2014).

3. – La pronuncia ha accertato che Deloitte, nel caso di specie, non possa ritenersi destinataria di dati personali, difettando di mezzi ragionevolmente accessibili idonei a consentire la re-identificazione degli interessati; ne consegue che, nei suoi confronti, le informazioni trasmesse debbano qualificarsi come dati anonimi. Diversamente, lo SRB, in quanto detentore delle chiavi di decodifica necessarie alla re-identificazione, trattava dati che conservavano inalterata la loro natura personale e, pertanto, avrebbe dovuto adempiere all'obbligo informativo verso gli interessati in ordine al trasferimento dei medesimi. Al punto 78 della sentenza, il quale fa esplicito riferimento al considerando 16 del Regolamento (UE) 2018/1725, si chiarisce che i dati *pseudonimizzati* rientrano comunque nella categoria dei dati personali, poiché, se esistono informazioni aggiuntive che permettono di risalire alla persona a cui tali dati si riferiscono, essi devono essere trattati come riferibili a un individuo identificabile. L'innovazione essenziale della sentenza in esame risiede nel porre il fulcro della valutazione di identificabilità non sul destinatario dei dati, bensì dal punto di vista del titolare del trattamento al momento della raccolta degli

DPCE online
ISSN: 2037-6677

stessi (punto 111). Viene, inoltre, sottolineato un particolare dalla CGUE che nella sua giurisprudenza più recente (Corte giust., sent. 09-11-2022, C-319/22, *Gesamtverband Autoteile-Handel e.V.*) ha ribadito che, ai fini della qualificazione di un'informazione come dato personale, non rileva esclusivamente la circostanza che essa sia conservata in forma *pseudonimizzata* o in chiaro, bensì occorre altresì considerare chi detiene il dato e quali risorse effettive abbia a disposizione per procedere alla re-identificazione (R. Streiber, D. Pöhn, *Legal and ethical considerations when conducting phishing experiments in Germany*, in 6 *Int. Cybersecur. Law Rev.* 245 (2025)).

La sentenza *OC c. Commissione europea* (Corte giust., sent. 07-03-2024, C-479/22 P) rappresenta un fondamentale punto di svolta nell'interpretazione della nozione di dato personale ai sensi dell'art. 3 sopracitato. La Corte ha chiarito che un'informazione deve considerarsi dato personale non solo in presenza di un'identificazione diretta dell'individuo, ma anche quando la sua identità possa essere desunta con una "probabilità ragionevolmente verosimile" attraverso l'incrocio di dati ulteriori facilmente accessibili (considerando 26 GDPR). L'accertamento dell'identificabilità non va, dunque, condotto sulla base della percezione di un generico "lettore medio", bensì tenendo conto delle concrete capacità e motivazioni di soggetti qualificati, in grado di operare una re-identificazione con mezzi proporzionati. Tale approccio conferma l'orientamento evolutivo della giurisprudenza europea, che privilegia la sostanza della tutela rispetto a criteri meramente formali di anonimizzazione, ponendo al centro la protezione effettiva dell'individuo contro i rischi di re-identificazione. La pronuncia si inserisce, peraltro, come anche la sentenza oggetto di questo contributo, nella tendenza del Tribunale verso un approccio relazionale alla nozione di dato personale, secondo cui la natura personale dei dati non è intrinseca, ma dipende dalla concreta possibilità, in capo al soggetto che li detiene, di ricondurli a un soggetto determinato (A. Lodie, *Case C-479/22 P, Case C-604/ /22 and the limitation of the relative approach of the definition of 'personal data' by the ECJ*, in *HAl open science*, 2024). Ne deriva che chiunque tratti dati *pseudonimizzati* deve dimostrare, in ossequio al principio di *accountability*, l'impossibilità materiale di re-identificare gli interessati, onde evitare l'applicazione della disciplina sui dati personali. Da qui il valore sistemico della pronuncia in esame, poiché segna un momento cruciale nella definizione dei confini della pseudonimizzazione ai sensi del Regolamento del 2018 e sollecita i legislatori e le istituzioni nazionali ad uniformarsi ai criteri interpretativi elaborati dalla Corte, promuovendo un approccio armonizzato e coerente alla tutela dei dati personali nell'Unione europea.

Diletta Sagliocco
Dipartimento di Scienze Politiche
Università degli Studi della Campania "Luigi Vanvitelli".
diletta.sagliocco@unicampania.it