Pseudonimizzazione e rischio di re-identificazione

Stefania Pia Perrino
Prof. a contratto dell'Università di Milano-Bicocca

Sommario: 1. Pseudonimizzazione e anonimizzazione. – **2.** L'identificabilità nella giurisprudenza europea. – **2.1.** La sentenza Breyer. – **2.2.** La sentenza Deloitte. – **2.3.** Le nuove coordinate della CGUE. – **3.** La nuova dimensione dell'identificabilità dell'interessato. – **4.** Dalla giurisprudenza alle riforme del *digital data acquis*. – **5.** Conclusioni.

1. Pseudonimizzazione e anonimizzazione

Pseudonimizzazione, cifratura e anonimizzazione sono misure di mitigazione del rischio di identificazione dell'interessato dal trattamento dei dati personali.

La pseudonimizzazione[1], tanto nel regolamento GDPR UE/2016/679 quanto nel regolamento UE/2018/1725 sul trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione europea, costituisce una delle strategie disponibili per la protezione dei dati personali: è una misura tecnica organizzativa che non trasforma il dato, ma si limita a ridurne la riconducibilità immediata all'interessato. Con questo

[1] Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale,* in *Riv. Trim. Dir. Proc. Civ.*, 2018, 2, 441-460, in particolare 445. Si vedano, inoltre, Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR,* in *Nuove Leggi Civili Commentate*, 2020, 2, 360-363; Pfitzmann-Dresden-Hansen, *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology,* 2010, 14 ss., disponibile al link: *https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.28.pdf*; Aggarwal-Yu, *Privacy-preserving Data Mining: Models and Algorithms*, New York, 2008; Codiglione, *Risk-based approach e trattamento dei dati personali*, in Sica-D'Antonio- Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, 67 ss.

meccanismo si rendono gli identificatori diretti non più attribuibili a una persona; ciononostante, i dati personali possono essere nuovamente riferiti all'individuo ricorrendo a una serie di informazioni aggiuntive[2]. La sicurezza della procedura risiede proprio nella separazione e successiva conservazione segregata delle informazioni aggiuntive rispetto al dato. In accordo con la nozione prevista dall'art. GDPR, la trasformazione citata può essere reversibile solo mediante l'uso di elementi esterni, a loro volta protetti da misure tecniche e organizzative adeguate, in modo da ridurre il rischio di identificazione, pur mantenendo la possibilità di ricondurre i dati all'interessato per finalità legittime.

Ancorché costituente una strategia per la protezione, si tratta di una forma di trattamento di dati personali; pertanto, non si esclude l'applicazione delle norme di protezione dei dati e trovano applicazione gli obblighi di liceità, trasparenza e sicurezza.

Per poter realizzare la pseudonimizzazione occorre seguire tre passaggi essenziali: mappatura, sostituzione e segregazione. In primo luogo, occorre rintracciare tutti gli identificatori, ossia i campi da sostituire e che potrebbero determinare l'identificazione dell'individuo, quali il nome, il codice fiscale, il numero di telefono oppure l'indirizzo e-mail. Successivamente, è necessario selezionare un meccanismo di sostituzione degli identificatori contenuti nei dati personali: si può procedere alla tokenizzazione oppure all'*hashing con sale* o *salting*, alla cifratura a chiave simmetrica o asimmetrica[3]. Infine, perché il meccanismo possa realizzare la sua funzione, occorre che sussista una barriera funzionante tra chiavi e riferimenti personali. Ciò può realizzarsi mediante una semplice archiviazione separata oppure con il controllo degli accessi o attraverso il *logging* o, ancora, con la rotazione delle chiavi. Inoltre, si rendono necessarie misure organizzative idonee a realizzare la separazione dei ruoli tra chi detiene la chiave e chi tratta i dati, procedure di accesso minimo e valutazioni d'impatto sulla protezione dei dati, specie quando la pseudonimizzazione è impiegata in trattamenti ad alto rischio.

Il mantenimento di un legame tra chiave ed identificativo, dunque la potenziale identificazione dell'interessato, rende questa tecnica preferibile quando è necessario mantenere un collegamento per finalità di ricerca, controllo o assistenza.

La cifratura è un'ulteriore misura tecnica di mitigazione del rischio, che diverge dalla pseudonimizzazione, in quanto funzionale alla tutela della riservatezza degli in-

---

[2] Ai sensi del 30° considerando GDPR, 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 – pur essendo di carattere pseudonimo – 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.

[3] Sulle misure, si vedano Faillace, *Il principio di privacy by design e di privacy by default*, in Bravo (a cura di), *Dati personali. Protezione, libera circolazione e governance*, Pisa, 2023, 466 ss.; Incerti, *Il principio di limitazione della finalità*, ivi, 193-194, 208, 220; D'orazio, *Protezione dei dati by default e by design*, in Sica-D'Antonio-Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, 79 ss.

teressati rendendo i dati personali illeggibili senza la chiave. La cifratura non modifica necessariamente la struttura identificativa dei dati, non elimina metadati e relazioni con gli identificativi, ma, similmente alla pseudonimizzazione, costituisce una procedura reversibile tramite decrittazione controllata.

La pseudonimizzazione va tenuta distinta[4] da e non costituisce un metodo di anonimizzazione[5]. Anche questa tecnica assurge a misura di mitigazione del rischio per la protezione del dato personali, tuttavia diverge perché è in grado di produrre dati impersonali, che non sono più riconducibili a una persona fisica sin dall'inizio oppure solo all'esito del trattamento. Mentre la pseudonimizzazione conserva una relazione con l'identificatore e costituisce un meccanismo potenzialmente reversibile da parte di chi ha il controllo delle chiavi, l'anonimizzazione non è reversibile e non residua alcun attuale o quantomeno potenziale riferimento all'individuo[6].

Perché sussista anonimizzazione deve ricorrere l'effettiva impossibilità di re-identificazione, tenuto conto dello stato di avanzamento tecnologico contingente, degli sviluppi successivi[7] e dello sforzo ragionevolmente applicabile per l'operazione[8].

Dalla distinzione tratteggiata precedentemente deriva una conseguenza cruciale per la qualificazione della misura adoperata: il dato sottoposto ad anonimizzazione non è mai stato oppure non è più un dato personale e risulta sottratto dal campo di applicazione del GDPR[9].

---

[4] Finocchiaro (a cura di), *Diritto all'anonimato*, in Galgano (a cura di), *Trattato di dir. comm e dir. pubbl. dell'economia*, XLVIII, Bologna, 2008; Id., *Anonimato,* in *Digesto disc. priv., Sez. Civ.,* Torino, 2010; Bolognini-Pelino-Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 74 ss.; Gaeta, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi,* in *Dir. dell'informazione e dell'informatica*, 2018, 1, 147-179, in particolare 161.

[5] Pellecchia, *op. cit.*, 362.

[6] Dall'analisi della prassi emerge però che non si può escludere in via assoluta la possibilità di identificazione mediante dato anonimizzato: in questo senso, si veda il Parere del Gruppo di lavoro per la protezione dei dati personali sulle tecniche di anonimizzazione, 10 aprile 2014, n. 5, in *www.ec.europa.eu*, nel quale si riporta come sia difficile creare dati effettivamente anonimi mantenendo tutte le informazioni necessarie per l'espletamento delle attività richieste. In dottrina, sul punto si rinvia a D'Orazio, *op. cit.*, 91; Bolognini-Pelino-Bistolfi, *op. cit.*, 77 ss.; Gaeta, *op. cit.*, 162.

[7] Nervi, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in Cuffaro-D'Orazio-Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 176.

[8] Sull'accezione relativa e non assoluta dell'impossibilità di re-identificazione, si veda Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, cit., 446. Sulla re-identificazione, si veda Foglia, *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in Panetta (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 e al novellato d.lgs. n. 196/2003, Torino, 2019, 309 ss.*

[9] In questo senso depone il Considerando n. 26 Reg. 2016/679/UE: «[...] 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. [...] I principi di protezione dei dati non dovrebbero pertanto 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

Così, la scelta tra pseudonimizzazione e anonimizzazione dipende dall'equilibrio tra utilità dei dati e rischio residuo: la seconda diviene l'opzione più indicata quando la conservazione di qualsiasi collegamento è superflua.

L'European Data Protection Board ha recentemente adottato le Linee Guida per la pseudonimizzazione, all'esito di periodiche consultazioni con diverse categorie di *stakeholders*. Le *best practices* precisano le modalità di attuazione della misura di mitigazione e introducono profili di interesse per lo studioso del diritto privato. In particolare, si afferma la pseudonimizzazione deve essere realizzata con misure adeguate, sia a livello organizzativo che contrattuale. I *Terms and conditions* devono contemplare la misura tra le clausole contrattuali e così, oltre ad ampliarsi l'oggetto dell'obbligo informativo precontrattuale, si individuano nuove prestazioni nell'accordo tra titolare e interessato dal trattamento. In secondo luogo, le linee guida si concentrano sulla reversibilità della misura: a differenza dell'anonimizzazione, la pseudonimizzazione può essere superata mediante l'accesso agli identificativi segregati dal titolare del trattamento oppure mediante attività di diversa natura. Quando si configura questo rischio avverso, occorre una notifica all'Autorità di vigilanza. Ciononostante, questo *data breach* deve essere segnalato solo nei casi in cui il titolare del trattamento disponga di sufficienti elementi per realizzare la comunicazione, senza un sacrificio eccessivo, e quando ritenga probabile la lesione dei diritti dell'interessato.

2. L'identificabilità nella giurisprudenza europea

Sia il regolamento GDPR sia il regolamento UE/2018/1725 recano una nozione di dato personale, consistente in un dato che reca informazioni che rendono l'interessato dal trattamento identificato o identificabile. Con un numero d'identificazione o grazie a uno o più elementi specifici caratteristici dell'identità fisica, fisiologica, psichica, economica, culturale o sociale, è possibile risalire alla persona fisica interessata dal trattamento dei dati.

Il dato personale che non sia stato sottoposto ad alcuna misura di mitigazione del rischio, come pseudonimizzazione o cifratura o anonimizzazione, dispone di elementi che consentono di risalire direttamente o indirettamente all'interessato e, per questa ragione, il dato deve essere trattato secondo le regole dei citati regolamenti. Quando sottoposto alle misure di protezione menzionate, invece, si può segregare o limitare l'accesso dei terzi a quegli elementi identificativi e, dunque, recidere il legame con l'interessato. Tuttavia, il dato è personale per chi tratta e può avere una diversa dimensione per il terzo. Difatti, il dato pseudonimizzato può essere un dato personale, se si considera la posizione del soggetto titolare del trattamento, che realizza la dissociazione tra cifra e identificatore e si fa garante di questa separazione. Tuttavia, il medesimo dato trasferito a un terzo può essere considerato impersonale ogniqualvolta il soggetto destinatario del dato non

---

l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca».

disponga dei mezzi per identificare. Altri terzi, invece, potrebbero avere accesso alle misure di mitigazione oppure a dataset che consentono di associare lo pseudonimo al dato, sicché il dato può essere impersonale per un terzo e personale per altri destinatari. Dunque, il concetto di identificabilità e il relativo rischio di identificazione dipendono dal soggetto che si considera nella vicenda specifica e dai mezzi di cui dispone tale soggetto.

Se quanto precede risulta chiaro nella prassi, non è così nella disciplina di legge. Difatti, il concetto normativo di identificabilità non è circoscritto e ciò ha generato una *querelle* interpretativa in seno alla Corte di Giustizia dell'Unione Europea lunga decenni e in via di risoluzione. Il pensiero corre al caso Breyer e al più recente e complesso *affaire* Deloitte.

2.1. La sentenza Breyer

Nel caso Breyer[10], la domanda di pronuncia pregiudiziale alla CGUE verteva sull'interpretazione del concetto di identificabilità, desumibile degli artt. 2, lett. a) e 7, lett. f) direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

La domanda è stata proposta nell'ambito di una controversia tra un cittadino tedesco, il sig. Patrick Breyer, e la Repubblica federale tedesca, in merito alla registrazione e alla conservazione, da parte di quest'ultima, dell'indirizzo IP riferibile al cittadino. In particolare, il sig. Breyer ha consultato vari siti Internet, accessibili al pubblico, dei servizi federali tedeschi per consultare informazioni aggiornate. Al fine di contrastare attacchi e consentire il perseguimento penale dei «pirati informatici», la maggior parte di questi siti registra gli accessi nei file di registro. In essi sono memorizzati, al termine della sessione di consultazione di tali siti, il nome del sito o del file consultato, le parole inserite nei campi di ricerca, la data e l'ora della consultazione, il volume dei dati trasferiti, il messaggio relativo all'esito della consultazione e l'indirizzo IP del computer a partire dal quale è stato effettuato l'accesso. L'interessato, dunque, lascia una sorta di impronta della propria consultazione, tramite gli indirizzi IP, ossia sequenze numeriche assegnate ai computer collegati a Internet, al fine di consentire la comunicazione tra i medesimi attraverso tale rete. L'indirizzo IP del computer che effettua l'accesso è trasmesso al

[10] Corte di Giustizia, sez. II, 19 ottobre 2016, C-582/14, Patrik Breyer c. Bundesrepublik Deutschland, in *EurLex*: «L'articolo 2, lettera a), della direttiva 95/46 del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, dev'essere interpretato nel senso che un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale ai sensi di detta disposizione, qualora detto fornitore disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive di cui il fornitore di accesso a Internet di detta persona dispone». Per un commento alla pronuncia, si vedano Pellecchia, *op. cit.*, 365 ss.; Zuiderveen Borgesius, *The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition,* in *European data protection Law Review*, 2017, 3, 130 ss.

server che ospita il sito consultato. Tale comunicazione è necessaria per inviare i dati richiesti al corretto destinatario. I fornitori di accesso a Internet assegnano ai computer degli utenti di tale rete un indirizzo IP che può essere o «statico» o «dinamico», ossia un indirizzo IP che cambia a ogni nuova connessione a Internet. A differenza degli indirizzi IP statici, gli indirizzi IP dinamici non consentirebbero di associare, attraverso file accessibili al pubblico, un dato computer al collegamento fisico alla rete utilizzato dal fornitore di accesso a Internet.

Ciò considerato, il sig. Breyer ha proposto un ricorso dinanzi ai giudici amministrativi tedeschi, chiedendo che alla Repubblica federale di Germania fosse inibito di conservare o far conservare da terzi, al termine delle sessioni di consultazione dei siti accessibili al pubblico di media online dei servizi federali tedeschi, l'indirizzo IP del nodo ospite, qualora tale conservazione risulti essere necessaria per finalità meritevoli di tutela. Si è posto, dunque, il problema dell'identificabilità del sig. Breyer.

Il rischio di re-identificazione tratteggia il discrimine tra dato personale e anonimo e, visto che non risulta adeguatamente individuato nella disciplina vigente, si sono sviluppate due diverse opzioni interpretative. Queste ricostruzioni sono state analizzate prima dalla Corte federale di giustizia tedesca e poi dalla Corte di Giustizia dell'Unione europea. Da un lato, si è sviluppata la tesi c.d. relativa, che considera la probabilità di identificabilità dell'interessato esclusivamente nella prospettiva del titolare del trattamento dei dati personali. Dall'altro lato, invece, è emersa la tesi assoluta oppure oggettiva, che considera l'identificabilità tenuto conto dei mezzi, dei fondi, delle tecnologie a disposizione del titolare del trattamento oppure di ogni altro terzo che diviene destinatario dei dati[11].

---

[11] Su entrambe le posizioni dottrinali, si vedano Esser-Kramer-von Lewinski (a cura di), *Kommentar zum Bundesdatenschutzgesetz. Nebengesetze*, IV ed., Colonia, 2014, 4-10; Nink-Pohle, *Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze*, in *Multimedia und Recht*, 2015, 9, 563-567; Heidrich-Wegener, *Rechtliche und technische Anforderungen an die Protokollierung von IT-Daten. Problemfall Logging,* in *Multimedia und Recht*, 2015, 8, 487-492; Leisterer, *Die neuen Pflichten zur Netz und Informationssicherheit und die Verarbeitung personenbezogener Daten zur Gefahrenabwehr*, in *Computer und Recht*, 2015, 10, 665-670. Sul dibattito occorre rinviare pure alla ricostruzione del *Bundesgerichtshof*: la Corte federale di giustizia ha espressamente richiamato la *querelle* dottrinale relativa alla scelta di un criterio «oggettivo» oppure di un criterio «relativo» al fine di stabilire se una persona sia identificabile. Applicando un criterio «oggettivo», dati come gli indirizzi IP, oggetto di discussione nel procedimento, potrebbero essere qualificati, al termine delle sessioni di consultazione dei siti Internet considerati, come dati personali anche qualora solamente un terzo sia in grado di determinare l'identità della persona interessata, terzo che, nel caso di specie, è il fornitore di accesso a Internet. Secondo un criterio «relativo», invece, dati siffatti potrebbero essere qualificati come dati personali nei confronti di un organismo, quale il fornitore di accesso a Internet, poiché consentono la precisa identificazione dell'utente, ma privi di tale qualificazione nei confronti di un altro organismo, quale l'operatore dei siti Internet consultati, dato che detto secondo diverso operatore non disporrebbe delle informazioni necessarie per identificarlo senza un eccessivo dispendio di risorse. Sul punto, è possibile pure richiamare il parere del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, 20 giugno 2007 n. 4, disponibile al link: https://ec.europa.eu/newsroom/article29/items/613101/en.

Per risolvere la controversia, la Corte di Giustizia muove dal contenuto della disciplina allora vigente e, segnatamente, dal testo del considerando 26 dir. 95/46, secondo il quale per determinare se una persona sia identificabile è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona. Nella misura in cui il considerando fa riferimento ai mezzi che possono essere ragionevolmente utilizzati tanto dal responsabile del trattamento quanto da altri, la sua formulazione suggerisce che, perché un dato possa essere qualificato come «dato personale» ai sensi dell'articolo 2, lettera a), di tale direttiva non si richiede che tutte le informazioni che consentono di identificare la persona interessata debbano essere in possesso di una sola persona, salvo che l'identificazione della persona interessata non risulti vietata dalla legge o praticamente irrealizzabile. Entro questa prospettiva, l'articolo 2, lett. a), dir. 95/46 dev'essere interpretato nel senso che un indirizzo IP dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale. L'identificabilità dipende, però, dal fatto che tale soggetto disponga di mezzi giuridici che gli consentano di far identificare la persona interessata grazie alle informazioni aggiuntive. Tuttavia, la CGUE ha precisato che l'art. 7, lett. f), dir. 95/46 osta a una normativa di uno Stato membro ai sensi della quale un fornitore di servizi di media online può raccogliere e impiegare dati personali di un utente di tali servizi, in mancanza del suo consenso, solo nella misura in cui detta raccolta e detto impiego siano necessari per consentire e fatturare l'effettiva fruizione dei suddetti servizi da parte dell'utente in questione, senza che l'obiettivo di assicurare il funzionamento generale dei medesimi servizi possa giustificare l'impiego di tali dati dopo una sessione di consultazione degli stessi.

Nel caso Breyer, la CGUE si pronuncia in maniera concisa sulla questione della identificabilità, lasciando però ancora aperto il dibattito.

2.2. La sentenza Deloitte

La pronuncia Deloitte interviene circa dieci anni dopo sull'art. 3 § 6 reg. UE/2018/1725, i cui contenuti sono equivalenti a quelli del GDPR, che ha a sua volta abrogato e sostituito la dir. UE/95/46. Nella parte argomentativa della pronuncia recentemente emessa dalla Corte di Giustizia, però, emergono osservazioni più precise per gli interpreti.

La vicenda prende avvio nel 2017, quando il Comitato di Risoluzione Unico (di seguito, CRU o SRB[12]) ha adottato un programma di risoluzione per il Banco Popular Espanol SA e, nell'occasione, ha incaricato la società di consulenza e revisione contabile, Deloitte, per lo svolgimento un'analisi comparativa tra il piano adottato e una procedura di insolvenza ordinaria, con lo scopo di verificare se gli azionisti e i creditori del Banco

[12] Acronimo di Single Resolution Board.

avrebbero potuto conseguire un miglior trattamento economico con la seconda opzione, così da corrispondere loro un indennizzo. Per adottare tale decisione, CRU ha dato un avviso sul sito internet e ha avviato il procedimento relativo al diritto di essere ascoltati: gli azionisti e i creditori avrebbero dovuto manifestare il loro interesse ad esercitare il diritto ad essere ascoltati, compilando un modulo di iscrizione online corredato dalla documentazione richiesta. È stata pubblicata l'informativa sul trattamento dei dati personali nell'ambito della procedura, successivamente è stata inviata un'e-mail con il link per accedere al modulo e, una volta conseguite le risposte, CRU ha chiesto a Deloitte di verificare che le proprie valutazioni risultassero ancora valide, considerate le osservazioni o quantomeno parte di queste conseguite dagli azionisti e creditori.

Nel 2019, alcuni degli azionisti e creditori hanno proposto reclamo per la violazione del regolamento UE 2018/1725, ossia il regolamento sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione. Secondo il reclamo, CRU non avrebbe informato gli interessati sulla trasmissione delle risposte al modulo a destinatari terzi, come la società di consulenza.

In un primo momento, il Garante Europeo della Protezione dei Dati (GEPD), ha riscontrato la violazione dell'art. 15 reg. 2018/1725, in virtù dell'inadempimento dell'obbligo informativo, e ha rivolto un ammonimento a CRU.

Nel 2020, CRU ha chiesto al garante di rivedere la propria decisione, tenuto conto del tipo di dati condivisi con Deloitte. Sicché il GEPD ha rivisto la propria decisione e ha affermato che i dati condivisi da CRU con Deloitte erano pseudonimizzati, dunque, insuscettibili di essere considerati personali per la limitatezza delle informazioni e dei mezzi per risalire all'identità, tuttavia, persiste l'inadempimento informativo poiché la società di consulenza era un destinatario di dati personali degli azionisti e creditori ma non risultava essere stata menzionata nell'informativa.

Nello stesso anno, CRU ha proposto un ricorso diretto contro la decisione del GEPD dinanzi al Tribunale europeo atteso che i dati condivisi non potevano costituire dati personali: il motivo di ricorso è stato accolto e la decisione controversa è stata annullata[13]. A sostegno di CRU, è stata autorizzata a intervenire la Commissione europea, mentre a sostegno del garante è intervenuto il Comitato europeo per la protezione dei dati.

La decisione è stata impugnata dal Garante europeo: il Tribunale avrebbe erroneamente escluso la natura personale dei dati e il rischio di re-identificazione sulla base di presunzioni. Diversamente, i dati condivisi da CRU concernevano le persone fisiche coinvolte, proprio perché recanti un punto di vista personale, e risultavano identificabili, visto che a ciascuna osservazione era associato un codice alfanumerico identificativo del creditore. In secondo luogo, il rischio di re-identificazione è stato valutato nella prospettiva del titolare al trattamento dei dati, ossia SRB; cionondimeno, la società di consulenza

[13] Trib. UE, sez. VIII, 26 aprile 2023, T-557/20, CRU c. Garante europeo della protezione dei dati, disponibile al link: *https://infocuria.curia.europa.eu/tabs/document?source=document&text=&docid=272910&pageIndex=0&doclang=IT&mode=lst&dir=&occ=first&part=1&cid=4441919*.

era in possesso dei dati e nulla ostava all'identificazione da parte di quest'ultima, neppure menzionata nell'informativa resa agli interessati.

La Corte interviene modificando e annullando parzialmente la pronuncia del Tribunale europeo.

La materia del contendere verte sulla violazione dell'art. 3, §§ 1 e 6, reg. 2018/1725[14], ossia del regolamento del Parlamento europeo e del Consiglio 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 dei dati. Disciplina e disposizione che, come si evince dalla premessa svolta dalla CGUE, hanno contenuto sostanzialmente analogo a quello del Regolamento sulla protezione dei dati personali e, segnatamente, all'art. 4 § 1 GDPR. Le specifiche previsioni menzionate hanno per oggetto la nozione di dato personale e quella di pseudonimizzazione, per verificare l'idoneità a sussumere entro tali definizioni pure le osservazioni sotto pseudonimo condivise con Deloitte.

Alla stregua dell'art. 3 § 1 reg. 2018/175, così come interpretato nei precedenti della Corte[15], costituisce dato personale una qualsiasi informazione concernente una persona fisica identificata o identificabile: si utilizza un'accezione estesa per comprendere ogni tipo di informazione, tanto oggettiva quanto soggettiva, anche sottoforma di pareri e valutazioni riguardanti l'interessato, considerando il contenuto, le finalità e l'effetto. Dunque, possono essere dati personali anche quelli contenuti in pareri e opinioni, visto che sono così strettamente connessi alla persona fisica, mentre non vale ad escludere tale natura il fatto che i dati siano rappresentati entro punti di vista personali. Ad esempio, costituiscono dati personali le correzioni apposte da un esaminatore a margine delle risposte scritte a un esame professionale, come già statuito nel caso Nowak[16].

Occorre verificare funzione e finalità di queste opinioni per pervenire a una qualificazione, sicché il Tribunale europeo è incorso in un errore di diritto allorquando ha

---

[14] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, 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.

[15] Corte di Giustizia, sez. I, 4 maggio 2023, C-487/21, F.F. c. Österreische Datenschutzbehörde, in *Eur-Lex.* Per un commento alla pronuncia, si vedano Keller-Spies, *EU: Scope of the fight of access persuant to art. 15 (3) GDPR – concept of the terms 'copy' and 'information'*, in *Computer Law Review International*, 2023, 3, 84 ss.; Ziemele, *Derecho de acceso del interesado a sus datos personales objeto de tratamiento: determinación de los conceptos de «copia» y de «información»,* in *La Ley Unión Europea*, 2023, 115.

[16] Secondo il dispositivo della Corte di Giustizia, sez. II, 20 dicembre 2017, C-434/16, Peter Nowak c. Data Protection Commissioner, in *Eur-Lex*: «L'articolo 2, lettera a), della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, deve essere interpretato nel senso che, in circostanze come quelle di cui al procedimento principale, le risposte scritte fornite da un candidato durante un esame professionale e le eventuali annotazioni dell'esaminatore relative a tali risposte costituiscono dati personali, ai sensi di tale disposizione».

omesso di considerare in concreto la natura di questi dati. Diverse considerazioni invece spende la CGUE sul rischio di re-identificazione in caso di pseudonimizzazione.

In accordo con le previsioni del GDPR e del reg. 2018/1725, non sono dati personali quelli anonimi oppure quelli resi sufficientemente impersonali in modo tale da impedire l'identificazione dell'interessato[17]. I dati pseudonimizzati non rientrano nella nozione di dato personale per diverse ragioni: non sono menzionati nella nozione autentica, ma semmai formano oggetto dell'art. 3 § 6 del regolamento. La pseudonimizzazione definita dalla menzionata previsione è un trattamento di dati non più attribuibili all'interessato senza l'utilizzo di informazioni aggiuntive e con la conservazione separata delle informazioni aggiuntive. La gestione segregata è presidiata da misure organizzative idonee a prevenire l'identificazione. La nozione presuppone l'esistenza di informazioni che consentono l'identificazione, tuttavia l'operatività delle misure citate può incidere sul carattere personale del dato.

L'esistenza di tali informazioni aggiuntive non determina da sé sola l'identificabilità. Occorre considerare in concreto, caso per caso, secondo un criterio di ragionevolezza, tutte le misure complessivamente adottate dal titolare del trattamento o dal terzo per verificare l'eventuale identificabilità dell'interessato. In particolare, è necessario valutare quei fattori oggettivi che concorrono a influenzare una simile procedura, come i costi, il tempo, le tecnologie disponibili al momento del trattamento e gli sviluppi tecnologici successivi, tutti necessari per realizzare l'identificazione nel caso concreto. Dunque, i dati pseudonimizzati possono essere dati personali ai fini della applicazione del regolamento menzionato così come alla stregua del GDPR; cionondimeno, a seconda dei casi, la pseudonimizzazione può impedire a persone diverse dal titolare del trattamento di identificare l'interessato. La nozione di dato personale per quanto volutamente ampia non è illimitata ed esclude dal suo spazio applicativo i dati impersonali.

Da questa serie di considerazioni la Corte ne fa discendere un'altra: se per il terzo destinatario non è possibile procedere all'identificazione allora non sussistono né il rischio di re-identificazione né un dato personale e, conseguentemente, non possono trovare applicazione in capo al soggetto terzo tutti quegli obblighi che i regolamenti associano al trattamento, tra cui l'obbligo di fornire adeguata, completa e chiara informazione all'interessato.

Si perviene così a valutare gli ulteriori profili di doglianza rilevati dal ricorrente: l'angolo prospettico entro cui si deve accertare l'identificabilità; il momento specifico in cui questa valutazione deve essere operata; lo spazio applicativo dell'obbligo di informazione. Difatti, l'art. 3 § 1 reg. 2018/1725 non precisa entro quale prospettiva è necessario valutare il rischio di re-identificazione. Sono altre le parti del regolamento che, invece, sembrano operare alcune precisazioni, tra cui il considerando n. 16, l'art. 15 e il considerando n. 35.

---

[17] Corte di Giustizia, Grande Sezione, 5 dicembre 2023, C-683/21, Nacionalinis visuomenes sveikatos centras prie Sveikatos apsaugos ministerijos c. Valstybinė duomenų apsaugos inspekcija, punto 57, in *Eur-Lex*.

Il terzo periodo del considerando 16 reg. 2018/1725 afferma che l'identificabilità deve considerare i fattori oggettivi e soggettivi, ossia i mezzi, i costi, l'avanzamento tecnologico, che possano essere adoperati con elevata probabilità dal titolare del trattamento o dal terzo, tenuto conto del trattamento, delle sue finalità, delle circostanze e del contesto specifico di applicazione.

L'art. 15 § 1 reg. 2018/1725 precisa che le informazioni sul trattamento devono essere fornite nel momento in cui i dati personali sono ottenuti, ossia al momento della raccolta[18], tenuto conto delle circostanze e del contesto specifici del caso[19], in forma concisa, trasparente, intellegibile e comprensibile[20].

Il considerando n. 35 prevede che devono essere precisate le conseguenze dell'eventuale rifiuto al trattamento dei dati, così da consentire all'interessato di decidere consapevolmente.

Come precisato poi dalla giurisprudenza in casi analoghi[21], peculiare è la funzione dell'obbligo informativo: le informazioni devono essere complete e dovrebbero certamente riguardare l'eventuale sussistenza di ulteriori destinatari dei dati, ma l'informativa serve all'interessato per pervenire a una decisione con cognizione di causa per acconsentire o rifiutare. Si vuole evitare una raccolta contro il consenso e il trasferimento a terzi contro la volontà dell'interessato.

Alla stregua di tali elementi, la Corte afferma che l'identificabilità deve essere valutata nella prospettiva del titolare del trattamento; sotto il profilo temporale, deve essere considerato il momento della raccolta dei dati; con riferimento all'obbligo di informazione di cui all'art 15 § 1 lett. d) reg. 2018/1725, esso si inserisce nel rapporto giuridico tra interessato e titolare, prima di eventuali trasferimenti a destinatari terzi; l'obbligo informativo sussiste a prescindere dalla qualificazione del dato come personale o meno all'esito della pseudonimizzazione.

---

[18] Corte di Giustizia, sez. II, 29 luglio 2019, C-40/17, Fashion ID GmbH & Co.KG contro Verbraucherzentrale NRWeV, in *Eur-Lex:* «Dal tenore letterale di tale disposizione (l'obbligo di informazione previsto all'articolo 10 della direttiva 95/46, ndr.) emerge che il responsabile del trattamento o il suo rappresentante deve fornire almeno le informazioni previste da tale disposizione alla persona presso la quale raccoglie i dati. Risulta quindi che tale informazione deve essere fornita dal responsabile del trattamento immediatamente, ossia al momento della raccolta dei dati».

[19] Corte di Giustizia, sez. IV, 11 luglio 2024, C-757/22, Meta Platforms Ireland c. undesverband der Verbraucherzentralen und Verbraucherverbände, in *Eur-Lex*: «L'importanza del rispetto di un siffatto obbligo di informazione è altresì confermata dal considerando 60 del GDPR, il quale enuncia che il principio del trattamento corretto e trasparente implica che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità, sottolineando che il titolare del trattamento dovrebbe fornire eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati».

[20] Sull'ampia accezione di dato personale nella giurisprudenza europea, si veda Mendola, *L'"intelligente" automazione nei sistemi di* credit scoring, in *Actualidad Jurídica Iberoamericana*, 2024, 20, 1128-1165, in particolare 1147.

[21] Corte di Giustizia, 29 luglio 2019, Fashion ID, cit., § 104.

Nella vicenda in esame, vero è che CRU ha fornito a Deloitte esclusivamente parte dei dati raccolti e pseudonimizzati, con una serie di misure volte a impedire l'identificazione, che non potevano essere superate o controllate dalla società di consulenza. Difettava in capo al terzo la possibilità di realizzare un controllo incrociato tra valutazioni dei creditori e azionisti recanti un codice alfanumerico e i dati identificativi degli interessati collegati a tali codici. Conseguentemente, la società non avrebbe potuto ragionevolmente, con i mezzi tecnici disponibili al momento della configurazione del trattamento, risalire all'identità e procedere alla re-identificazione. Cionondimeno, l'identificabilità dell'interessato non deve essere valutata nella prospettiva del terzo, bensì del titolare del trattamento, tenuto conto delle finalità e del momento di raccolta allorquando deve essere adempiuto l'obbligo informativo *ex* art. 15 reg. 2018/1725: nel caso di specie, SRB disponeva di tutte le informazioni per identificare gli azionisti e i creditori, nonostante la pseudonimizzazione risultava possibile risalire all'identità e, dunque, possono essere considerati come dati personali.

2.3. Le nuove coordinate della CGUE

La decisione Deloitte, più complessa e più articolata del precedente Breyer, circoscrive la nozione di dato personale, anche se ne mantiene le sue geometrie variabili. In particolare, anche le osservazioni e le opinioni possono costituire dati personali al pari di nome, cognome, numero di telefono e indirizzo e-mail. Questi dati, una volta sottoposti al trattamento di pseudonimizzazione, possono continuare a rientrare nella categoria dei dati personali, ma non sempre: infatti, diventano impersonali e ne seguono il regime giuridico, se chi li riceve da altri non ha accesso alle chiavi e agli strumenti per realizzare la re-identificazione.

Con riferimento alla re-identificazione, si ribadisce l'adesione al criterio elaborato nel caso Breyer: l'identificabilità dell'interessato deve essere valutata dal punto di vista del soggetto che realizza il trattamento e si pongono al centro i meccanismi di *risk assessment* adoperati. Occorre, dunque, considerare il rischio senza automatismi: deve riscontrarsi l'impossibilità materiale e legale di associazione tra informazioni supplementari e pseudonimo o, se il rischio sussiste, deve essere insignificante, tenuto conto dei fondi e delle tecnologie che possono essere adoperate concretamente e ragionevolmente da parte di chi detiene il dato pseudonimizzato.

La pronuncia, poi, precisa meglio i confini degli obblighi informativi, cui è tenuto il titolare del trattamento, specie per i casi in cui il dato personale risulti successivamente sottoposto alle misure di mitigazione del rischio prima analizzate. L'informazione costituisce uno degli elementi strutturali del rapporto giuridico tra titolare e interessato: il primo rende consapevole il secondo sulle modalità di utilizzo del dato e orienta quest'ultimo nella scelta di prestare o meno il successivo consenso al trattamento e all'eventuale trasferimento. L'obbligo è posto in capo al titolare del trattamento, in forma concisa, trasparente, intellegibile, accessibile, tenuto conto del momento in cui i dati sono raccolti e prima di eventuali trasferimenti a terzi. Dunque, anche se eventualmente e successivamente un terzo riceve dei dati sottoposti a pseudonimizzazione e pertanto non sono ri-

feribili all'interessato secondo il criterio Breyer, applicato in concreto, l'obbligo di informazione di cui all'art. 15 § 1 lett. d) reg. UE/2018/1725 impone al titolare del trattamento di informare comunque l'interessato sui destinatari del trasferimento dei suddetti dati.

3. La nuova dimensione dell'identificabilità dell'interessato

La riconfigurazione del concetto di identificabilità e del rischio di re-identificazione hanno destato sin da subito l'attenzione degli interpreti per la possibilità, in passato avvertita come frustrata, di determinare una contrazione della nozione ampia di dato personale. Si favorirebbe così una più agile circolazione dei dati previa pseudonimizzazione. Cionondimeno, la decisione desta alcune perplessità e appare rilevante pure per altre ragioni.

La nozione di dato personale non si restringe o allarga in via astratta e assoluta: potenzialmente, l'applicazione di tecniche di cifratura, pseudonimizzazione e anonimizzazione può determinare il superamento del rischio di re-identificazione, specie considerando i mezzi che il soggetto può concretamente adoperare. Tuttavia, l'adesione al criterio Breyer determina ricadute applicative importanti: la valutazione concreta dovrà considerare tutte le nuove e sofisticate tecnologie disponibili al momento del trattamento, che possono essere utilizzate per risalire all'interessato, ancorché si debbano considerare solo quelle concretamente adoperabili dal titolare o dal terzo per la re-identificazione. Dunque, se in concreto si può considerare in via di restrizione la nozione di dato personale, l'identificabilità può considerarsi oggi sottoposta ad ampliamento o contrazione a seconda degli avanzamenti della tecnica. Questo orientamento allora introduce un livello di peculiare complessità nella valutazione richiesta e, peraltro, ciò non costituisce un rischio eminentemente teorico: l'analisi della prassi ha già restituito agli interpreti un quadro che depone nel senso dell'estensione dello spazio di identificabilità dei dati ancorché sottoposti a misure di mitigazione. Secondo il Parere del Gruppo di lavoro per la protezione dei dati personali sulle tecniche di anonimizzazione[22], non si può escludere in via assoluta la possibilità di identificazione e, allo stato attuale, è assai difficile creare dati effettivamente anonimi mantenendo segregate tutte le informazioni necessarie per l'espletamento delle attività richieste.

In secondo luogo, nella sentenza sembra evidenziarsi un cortocircuito, che pare stonare con l'adesione al criterio Breyer. Secondo la CGUE, i dati personali possono diventare impersonali e viceversa: i dati pseudonimizzati non costituiscono, in ogni caso e per qualsiasi persona, dati personali ai fini dell'applicazione dei regolamenti GDPR e 2018/1725. In caso di pseudonimizzazione occorre verificare in concreto la disponibilità degli strumenti giuridici per ottenere da altri le informazioni aggiuntive per procedere all'identificazione,

[22] In questo senso, si veda il Parere del Gruppo di lavoro per la protezione dei dati personali sulle tecniche di anonimizzazione, 10 aprile 2014, n. 5, in www.ec.europa.eu. In dottrina, sul punto si rinvia a D'Orazio, *op. cit*., 91; Bolognini-Pelino-Bistolfi, *op. cit*., 77 ss.; Gaeta, *op. cit*., 162.

considerando i costi, il tempo, le tecnologie disponibili al momento del trattamento e gli eventuali sviluppi tecnologici. Tuttavia, al § 85 la Corte stigmatizza l'operato del Garante europeo della protezione dei dati perché, nel censurare la condotta di CRU, ha riscontrato un astratto rischio di re-identificazione in caso di eventuale controllo incrociato e ha affermato che i dati pseudonimizzati dovrebbero costituire dati personali sottoposti alla disciplina del GDPR sia nel trasferimento alla società di consulenza sia nel trasferimento ulteriore ad eventuali altri destinatari. Difatti, si legge espressamente: «quest'ultimo deve essere considerato identificabile per quanto riguarda tanto tale trasferimento quanto qualsiasi ulteriore trattamento di tali dati da parte di detti terzi. In tali circostanze, i dati pseudonimizzati dovrebbero essere considerati personali». Dunque, la conclusione dei giudici europei è quella di imporre sempre una verifica in ordine alla sussistenza o meno di rischio di re-identificazione da parte di persone diverse dal titolare del trattamento; ciononostante, poi si afferma che una volta riscontrato il pericolo concreto di controllo incrociato o di ogni altra modalità di associazione delle chiavi agli identificatori allora il dato diviene personale sempre e comunque nei fenomeni circolatori successivi. Al contrario, si dovrebbe affermare che il dato può essere considerato impersonale in caso di trasmissione a un terzo che non dispone di strumenti per risalire all'identità, ma può tornare a essere personale e può configurarsi una re-identificazione dell'interessato quando un diverso destinatario dispone di strategie idonee per superare la dissociazione, ad esempio svolgendo un controllo incrociato con un proprio ampio *data set*.

Infine, le precisazioni offerte nel caso Deloitte potranno determinare un effetto agevolatore per la circolazione dei dati, specie in un contesto come quello contingente caratterizzato dall'uso massivo di *big data* per alimentare i sistemi di intelligenza artificiale. Ciononostante, questa particolare attitudine deriva dal momento in cui questa pronuncia è stata adottata, ossia in un periodo di profonde riforme in ambito europeo, che concorrono a comporre «"il diritto europeo dei dati" e quindi dell'"European Data Strategy"»[23].

4. Dalla giurisprudenza alle riforme del *digital data acquis*

A favorire l'innovazione e la competitività dell'Unione europea[24] è recentemente intervenuto, infatti, l'*European Health Data Space* (di seguito, EHDS). Specialmente dopo la pandemia, l'Unione Europea ha adottato una serie di discipline volte a rafforzare la protezione dei dati personali in modo compatibile però con una maggiore disponibilità di dati sanitari in grado di supportare i protocolli di ricerca e la crescita economica. Tra

[23] Caso-Guarda, *Ricerca e Spazio Europeo dei Dati Sanitari tra regole proprietarie e apertura*, in *Accademia*, 2025,837-850.

[24] Sulle diverse iniziative in materia, si veda Morace Pinelli (a cura di), *Dalla Data Protection alla Data Governance: il Regolamento (UE) 2022/868*, Pisa, 2024; Id., *Data Act. Introduzione interdisciplinare e commentario al regolamento (UE) 2023/2854*, Pisa, 2025; Id., *la circolazione dei dati personali: persona, contratto e mercato*, Pisa, 2022.

queste spicca l'EHDS[25], che ha recentemente introdotto due binari di circolazione dei dati personali in ambito sanitario: il primo riguarda i dati sanitari a uso primario, che continuano a essere sottoposti al regime fondato sul consenso informato, e un secondo binario relativo ai dati per uso secondario, accessibili senza un previo consenso, purché il trattamento risulti funzionale al perseguimento di definite finalità di pubblico interesse *ex* art. 53 EHDS[26]. Non solo, perché il consenso informato autorizzativo al trattamento dei dati da regola diviene eccezione: la circolazione dei dati sanitari elettronici avviene senza necessità del consenso espresso da parte dell'interessato per il trattamento, salvo l'esercizio del diritto di opposizione o di esclusione[27].

Quelli cui fa riferimento l'EHDS, però, sono dati relativi alla salute degli individui ed elettronici, tipicamente rinvenibili nei fascicoli sanitari. Semmai, per quanto qui interessa, il regolamento introduce espressamente nuovi divieti di trattamento che concorrono ad ampliare la nozione di dato personale.

Con riferimento, invece, alla generalità dei dati, è necessario considerare una rilevante recente proposta, che potrebbe essere idonea a recepire le coordinate della sentenza Deloitte, ossia la proposta c.d. *Digital Omnibus*.

Il *Digital Omnibus*[28] costituisce un insieme di proposte legislative della Commissione Europea, avanzato nel novembre 2025. Con questa proposta si intende razionalizzare, armonizzare e semplificare l'intero quadro normativo digitale dell'UE, con modifiche

---

[25] Morace Pinelli, *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025),* in *Nuova Giurisprudenza Civile Commentata*, 2025, IV, 1016-1031, in particolare 1020; Faccioli, *La responsabilità civile per violazione della disciplina per l'utilizzo dei dati sanitari elettronici nell'European Health Data Space (art. 100 Reg. 2025/327/UE),* in *Resp. civ. prev.,* 2025, 5; V. Ricciuto, *Una circolazione dei dati sanitari anche nella prospettiva del mercato?,* in questa *Rivista*, 2025, 9, 823-836; Caso-Guarda, *op. cit*., 837-850; Faillace, *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo regolamento EHDS,* in *Contratto e Impresa*, 2025, 2, 379-401; Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327,* in *Nuove Leggi Civili Commentate,* 2025, 3, 563-603; Id., *Il trattamento dei dati personali in ambito sanitario,* in *Riv. it., informatica e diritto*, 2025, 2, 2-20; Cascini-Arcuri, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale,* in *Diritto dell'informazione e dell'informatica*, 2024, 6, 837 ss.; Zambrano, *EHDS e soggetti vulnerabili: tra esigenze di condivisione dei dati sanitari e tutela della persona*, in *Accademia*, 2025, 1097.

[26] Tra queste si annoverano sanità pubblica e medicina del lavoro, ma anche politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, statistiche, attività d'istruzione o d'insegnamento nel settore sanitario, ma pure ricerca scientifica nel settore sanitario o dell'assistenza. Sull'accezione pubblicistica della disciplina e dell'accesso ai dati a uso secondario, si veda Ricciuto, *op. cit.*, 834.

[27] In questo senso, si veda Ricciuto, *op. cit*., 829.

[28] Proposta di Regolamento del Parlamento europeo e del Concilio per la modifica dei Regolamenti 2016/679, 2018/1724, 2018/1725, 2023/2854 e delle Direttive 2002/58, 2022/2555 e 2022/2557 per la semplificazione del quadro normativo digitale, e per l'abrogazione dei Regolamenti 2018/1807, 2019/1150, 2022/868, e della Direttiva 2019/1024 (Digital Omnibus).

a GDPR, AI Act[29], Data Act[30] e NIS2[31], per ridurre gli oneri amministrativi e allineare la regolamentazione alle esigenze di innovazione dei settori coinvolti, considerata la complessità ormai raggiunta dal *data legislative aquis.*

Per quanto qui interessa, secondo il Considerando n. 27, il regolamento propone una serie di modifiche per il GDPR. In particolare, si intende intervenire sul tenore dell'art. 4 GDPR relativo alla nozione di dato personale, ossia l'informazione o le informazioni su una persona identificata o identificabile. La proposta prevede una precisazione in ordine al concetto di identificabilità: dovrebbero essere considerati tutti i mezzi che ragionevolmente potrebbero essere utilizzati per identificare direttamente o indirettamente una persona. Proprio in accordo con le coordinate offerte nelle vicende Breyer e Deloitte, l'esistenza di informazioni aggiuntive segregate rispetto al dato non determina che esso risulti necessariamente personale; sicché il dato pseudonimizzato non rientra di per sé nello spazio di applicazione del regolamento GDPR. Semmai occorre chiarire che il dato non può essere considerato come personale quando l'ente che lo tratta non dispone degli strumenti idonei per svolgere il controllo incrociato tra chiavi ed identificativi. Dunque, anche la proposta aderisce al criterio Breyer. Conformemente, la nozione di dato personale e il concetto di identificabilità devono escludere dal loro campo di applicazione i casi in cui il rischio di identificazione appaia in realtà insignificante, o perché l'identificazione di tale interessato è vietata dalla legge o quando risulti impossibile nella pratica o, ancora, perché comporterebbe uno sforzo sproporzionato in termini di tempo, costi e manodopera. Si menziona, poi, espressamente un esempio di divieto di re-identificazione, che si trova poi proprio nel citato regolamento EHDS e, segnatamente, tra gli obblighi degli utenti dei dati sanitari di cui all'articolo 61, § 3, reg. 2025/327.

In via ulteriore, il considerando n. 27 precisa quanto previsto nel § 85 della sentenza Deloitte. Secondo la proposta, una potenziale trasmissione successiva a terzi delle informazioni sottoposte a misura di pseudonimizzazione, rende tali informazioni dati personali solo per quei terzi che dispongono dei mezzi che consentono loro di identificare ragionevolmente la persona fisica cui si riferiscono le informazioni. Si evitano così i dubbi determinati dal confronto tra l'adesione al criterio Breyer e la formulazione del § 85 della pronuncia.

---

[29] Regolamento 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 recante le coordinate per l'armonizzazione delle regole sull'intelligenza artificiale, G.U. 12 luglio 2024. Sul punto, è necessario menzionare che l'Italia ha adottata la prima disciplina in Europa per la regolazione dell'intelligenza artificiale, con la Legge 23 settembre 2025, n. 132, recante *Disposizioni e deleghe al Governo in materia di intelligenza,* in G.U. 25 settembre 2025, n. 223, entrata in vigore in data 10 ottobre 2025.

[30] Regolamento 2023/2854 del Parlamento europeo e del Consiglio del 13 Dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati), G.U. 22 dicembre 2023.

[31] Direttiva 2022/2555 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante la modifica del regolamento n. 910/2014 e della direttiva 2018/1972 e che abroga la direttiva 2016/1148.

5. Conclusioni

Il periodo storico contingente è caratterizzato ormai da un uso massivo di dati, specie per il funzionamento di macchine e sistemi automatizzati, da impiegare in medicina, in ambito educativo, negli acquisti, nello sport e ogni altro settore interessato. La circolazione di questi dati, però, deve fare i conti con la notevole disciplina introdotta dall'Unione Europea per la protezione degli interessati da utilizzi vietati e forme di abuso rispetto a questi dati.

Tra le forme più frequenti di protezione si annovera la pseudonimizzazione, intesa come separazione tecnica di identificatori diretti e indiretti mediante chiavi o codici. Si riduce la probabilità di identificazione immediata, ma non si esclude la possibilità, in presenza di informazioni accessorie o di capacità tecniche avanzate, di re-identificare l'interessato.

La pseudonimizzazione non è idonea di per sé a rendere il dato personale o impersonale. Ciò dipende dal soggetto considerato nella valutazione del rischio di re-identificazione. Il titolare del trattamento dispone dell'accesso a quelle informazioni, ma un terzo destinatario del dato pseudonimizzato potrebbe non avere questo tipo di autorizzazioni oppure, al contrario, potrebbe disporre di mezzi economici e tecnici tali da poter superare le barriere citate e risalire all'identità dell'interessato. La valutazione del rischio di re-identificazione, come suggeriscono la prassi e le linee guida, deve considerare non solo la natura del dato e le tecniche applicate, ma anche il contesto di diffusione, i destinatari potenziali, le risorse economiche e tecnologiche a disposizione di terzi e le misure organizzative e contrattuali adottate dal titolare. La qualificazione del dato come personale o non personale non può essere stabilita a priori in modo assoluto, ma richiede un'analisi fattuale e prospettica.

Per questo si è reso necessario circoscrivere e precisare i confini del concetto di identificabilità, solo presupposto e abbozzato nelle diverse discipline europee intervenute sul punto, ivi compreso il GDPR. La Corte di Giustizia dell'Unione europea, prima nel caso Breyer poi nel caso Deloitte, cerca di superare la *querelle* interpretativa ed aderire a un modello fondato su valutazioni pragmatiche e funzionali, da svolgere in concreto nella prospettiva di chi tecnicamente tratta il dato.

La rilevanza di queste pronunce si fa oggi ancora più evidente, perché si consente di far circolare dei dati senza dover fare applicazione delle numerose e talvolta assai macchinose garanzie previste dal GDPR, a vantaggio di un'economia ormai fondata sui numerosi, aggiornati, sofisticati *set* di dati.

L'impatto non è solo indirettamente economico ma anche direttamente giuridico, atteso che le nuove proposte di riforma prendono atto delle coordinate interpretative della Corte di Giustizia e mirano alla riforma del regolamento GDPR in conformità. A questo punto, la CGUE ha tratteggiato un solco rilevante per il *risk assessment* che dovrà essere realizzato ogni volta al fine di stabilire se risulti o meno applicabile il GDPR allo specifico trattamento, tuttavia bisognerà verificare se il disegno sarà compiuto con l'adozione del *Digital Omnibus* e con la riforma della nozione di dato personale.

Abstract

La pseudonimizzazione sostituisce gli identificatori diretti con chiavi, riducendo i rischi di circolazione ma mantenendo la natura di dato personale per chi può accedere ai meccanismi di collegamento. Tuttavia, il GDPR non definisce l'"identificabilità", generando incertezza applicativa del Digital Data Acquis. La CGUE ha progressivamente elaborato criteri per valutare identificabilità e rischio di re-identificazione, influenzando le recenti riforme europee in materia di protezione dei dati e governance digitale. Il saggio analizza l'evoluzione del concetto di identificabilità e le sue implicazioni regolatorie.

Pseudonymisation replaces direct identifiers with codes to limit risks in data circulation, yet data remain personal under the GDPR for anyone able to access the linking keys. The Regulation, however, offers no definition of identifiability, creating uncertainty across the EU's digital acquis. Different rulings of the Court of Justice have progressively shaped criteria for assessing identifiability and re-identification risks. These judicial approaches are influencing recent EU reforms on data protection and digital governance. This essay analyses the evolving notion of identifiability and its implications for current regulatory frameworks.