Le linee guida dell'European Data Protection Board (EDPB), n. 02/2026 sull'anonimizzazione dei dati

14/09/2026 PROTEZIONE DEI DATI E CYBERSECURITY

Roberto A. Jacchia
Camillo Campli
Anna Chiara Frascari

Il parere n. 05/2014 del Gruppo di lavoro "Articolo 29" sulle tecniche di anonimizzazione aveva fornito, a suo tempo, tre criteri per valutare l'anonimato dei dati: (i) isolamento/individuazione: la possibilità di isolare o distinguere una persona o un dato all'interno di un insieme di dati; (ii) collegabilità: la possibilità di collegare tra loro due o più dati riferiti alla stessa persona o allo stesso gruppo di persone, anche provenienti da dataset diversi; (iii) inferenza: la possibilità di dedurre, con una probabilità significativa di successo, un'informazione relativa a una persona a partire da altri dati disponibili.

Pur avendo costituito per oltre un decennio il principale riferimento in materia, l'evoluzione della giurisprudenza della Corte di giustizia dell'Unione europea (CGUE), lo sviluppo, a livello unionale, di quadri e infrastrutture comuni per la condivisione e il riutilizzo dei dati e gli sviluppi registrati tanto nel campo dell'intelligenza artificiale quanto in quello tecnologico in generale, hanno reso necessario aggiornare tale parere. Sotto il profilo giurisprudenziale, assume particolare rilievo la sentenza della CGUE del 4 settembre 2025 (causa C-413/23 P, nota come sentenza "Deloitte"), che ha evidenziato la necessità di definire una architettura strutturata per la valutazione del rischio di re-identificazione. Le Linee Guida n. 02/2026 sull'anonimizzazione, adottate il 7 luglio 2026 dall'EDPB costituiscono tale aggiornamento, perfezionando i criteri già elaborati e introducendo nuove indicazioni specifiche e consentendo, ove possibile e proporzionato, un utilizzo dei dati che tenga conto e tuteli al contempo i diritti delle persone fisiche.

Il cuore dell'analisi elaborata dall'EDPB si articola attorno a due quesiti fondamentali: se l'informazione riguardi o meno una persona fisica e, se quella persona sia o meno identificata o identificabile. Se la risposta a una delle due domande è no, il dato è da

considerarsi anonimo. Tuttavia, si deve sottolineare che la risposta alla seconda domanda non può essere assoluta, ma da valutare caso per caso. Per determinare quali siano le prospettive rilevanti, è necessario esaminare la natura specifica e il contesto del trattamento, in particolare chi vi abbia accesso o ne detenga il controllo, se i dati vengono trasmessi, il rapporto tra le parti interessate e se il soggetto che riceve i dati li tratti per conto di un'altra parte.

Su quest'ultimo aspetto, le Linee Guida sono esplicite: se un soggetto "A" tratta dati per conto di un titolare del trattamento "B", tali dati devono essere considerati personali anche per il soggetto A che li elabora, il quale deve pertanto essere qualificato come responsabile del trattamento ai sensi del GDPR ed essere assoggettato ai relativi obblighi. Ciò, per impedire che i titolari eludano le tutele del Regolamento esternalizzando le loro attività di trattamento a soggetti terzi. Per determinare se un'informazione possa essere considerata riferita a una persona fisica, è necessario valutare il legame tra l'informazione e l'interessato alla luce di tutte le circostanze del caso concreto: la riferibilità può essere dedotta per ragioni di contenuto, scopo o effetto. Sotto il primo profilo, un'informazione è riferibile a una persona in ragione del proprio contenuto quando descrive direttamente l'individuo, oppure ne identifica o richiama caratteristiche, comportamenti o attività. La riferibilità può anche derivare dallo scopo perseguito attraverso l'utilizzo dell'informazione. Ciò si verifica quando il dato, pur avendo ad oggetto un bene, un'organizzazione o un altro soggetto collegato all'interessato, viene impiegato per valutarne la posizione, determinarne il trattamento o orientarne il comportamento. Infine, il collegamento con la persona può essere individuato in funzione degli effetti prodotti. In questo caso, l'informazione può riguardare direttamente un bene, un'organizzazione o un altro individuo, ma il suo trattamento è comunque suscettibile di incidere concretamente sulla posizione giuridica o sugli interessi dell'interessato, determinando la possibilità che quest'ultimo venga trattato in maniera differente rispetto ad altri soggetti.

Successivamente, occorre stabilire se la persona sia identificata o identificabile. Identificare una persona significa distinguerla dalle altre in un determinato contesto, così da poterla sottoporre a un trattamento differenziato. Ciò può avvenire mediante identificazione diretta o indiretta: un individuo è direttamente identificabile quando il soggetto che dispone dell'informazione è già in grado, attraverso i mezzi a propria disposizione, di ricondurla a una persona determinata. È il caso, ad esempio, delle informazioni che riportano il nome dell'interessato oppure un identificativo univoco, quale un numero di codice o un riferimento personale. L'identificazione è invece indiretta quando la riconducibilità del dato a una persona richiede il ricorso a ulteriori elementi o strumenti. Ciò può verificarsi, ad esempio, quando occorre acquisire informazioni detenute da altri soggetti, ricorrere a procedure tecniche gestite da terzi oppure combinare il dato con altre informazioni nella disponibilità di soggetti diversi. In tale prospettiva assume particolare rilevanza la nozione di "catena di mezzi", secondo cui la possibilità di identificare una persona deve essere valutata considerando anche la possibilità di integrare risorse e informazioni distribuite tra più soggetti. Non è quindi necessario che un'unica entità disponga autonomamente di tutti gli elementi necessari alla re-identificazione: è sufficiente che questi possano essere ragionevolmente messi in relazione o combinati attraverso strumenti concretamente accessibili.

Questa impostazione incide direttamente sulla qualificazione dei dati. Qualora un soggetto trasferisca i dati a un terzo capace di re-identificare gli interessati, non si può escludere la natura personale dei dati sulla base della sola incapacità del cedente di procedere autonomamente alla loro identificazione. I dati possono, infatti, mantenere tale carattere sia nell'ambito del trasferimento sia rispetto al successivo trattamento effettuato dal destinatario e, per la medesima ragione, possono essere considerati dati personali anche dal punto di vista del soggetto che li ha trasferiti.

Il concetto di "mezzi ragionevolmente utilizzabili" è centrale nell'intera architettura del framework. Piuttosto che enumerare i mezzi che potrebbero condurre all'identificazione, le Linee Guida ne definiscono i confini negativi: un

mezzo può non essere considerato ragionevolmente utilizzabile qualora la sua realizzazione sia impossibile, richieda uno sforzo sproporzionato in termini di tempo, costi o lavoro, oppure sia vietato dalla legge. La valutazione della probabilità che un soggetto impieghi determinati mezzi deve essere condotta alla luce di tutti i fattori oggettivi rilevanti. Tra questi, le Linee Guida annoverano: le caratteristiche del dato (grado di aggregazione, unicità dei record, accuratezza e precisione delle informazioni), e il modo in cui tali caratteristiche possono incidere sulla possibilità di risalire agli interessati con i diversi possibili metodi di re-identificazione; il contesto in cui i dati sono rilasciati e/o trattati, ivi compresa la presenza di restrizioni effettive e permanenti all'accesso; le informazioni aggiuntive che potrebbero consentire l'identificazione degli individui e la probabilità di ottenerle; i costi e il tempo necessari per acquisirle; la tecnologia disponibile al momento del trattamento e i prevedibili sviluppi tecnologici futuri; l'obsolescenza dei dati e la loro collocazione nel tempo, poiché il trascorrere del tempo può incidere sulla loro accuratezza e sulla possibilità di collegarli a ulteriori informazioni disponibili.

Sotto il profilo soggettivo, il GDPR non pone alcuna condizione in merito ai soggetti in grado di identificare l'individuo. I soggetti rilevanti comprendono chiunque riceva i dati, direttamente o indirettamente, ivi inclusi soggetti non autorizzati e operanti illegalmente. A seconda delle circostanze, tra questi possono figurare: il titolare del trattamento dei dati da anonimizzare; i soggetti destinatari; i dipendenti (anche "infedeli"); i partner, gli amici, i colleghi e i familiari degli interessati; i giornalisti investigativi; le autorità di polizia o i servizi di intelligence nazionali o stranieri; le imprese prive di scrupoli; i cybercriminali.

Una volta definito il perimetro dei soggetti rilevanti, le Linee Guida affrontano alcune questioni di particolare delicatezza. Anzitutto, l'EDPB mette in guardia dall'utilizzare la mancanza di un movente alla re-identificazione come elemento escludente il relativo rischio, in quanto la motivazione di un soggetto è difficile da accertare e valutare oggettivamente, può mutare nel tempo e le sue azioni possono non essere coerenti con lo stesso. La re-identificazione può, del resto, verificarsi anche accidentalmente, per negligenza o per effetto di circostanze esterne che costringano un soggetto ad identificare un individuo o a trasferire informazioni che lo consentano.

Nella medesima prospettiva, nella valutazione dei mezzi ragionevolmente utilizzabili, occorre tenere conto del valore potenziale dei dati re-identificati per chi effettua la re-identificazione, valore che non si esaurisce nella dimensione economica.

Quanto al ruolo dei divieti legali, la CGUE ha affermato che i mezzi vietati dalla legge non devono essere considerati qualora la probabilità del loro utilizzo sia nella realtà insignificante. Tale conclusione presuppone tuttavia che i soggetti coinvolti siano effettivamente vincolati dallo Stato di diritto, così che il divieto risulti concretamente efficace. La presunzione generale di rispetto della legalità può essere superata qualora sussistano prove sufficienti di un rischio concreto che vengano comunque impiegati mezzi illeciti. La valutazione deve tenere conto, in particolare, dell'effettiva capacità di controllare il rispetto del divieto e di sanzionarne le violazioni; dell'eventuale convenienza per i soggetti interessati a violarlo, qualora i vantaggi ottenibili risultino superiori ai costi e ai rischi derivanti dalla condotta illecita; della vulnerabilità dei dati utilizzabili per la re-identificazione rispetto a possibili accessi non autorizzati; nonché dell'esistenza di precedenti episodi di violazione o aggiramento del divieto in circostanze analoghe. Su questo punto si innesta un'ulteriore precisazione di rilievo pratico: un divieto stabilito contrattualmente, quindi giuridicamente vincolante tra le parti, non può essere equiparato a un divieto di legge. Le clausole contrattuali di riservatezza possono avere un'incidenza sui mezzi ragionevolmente utilizzabili, ma devono essere intese unicamente come complemento alle misure tecniche e non come autonomo strumento di anonimizzazione, tenuto conto che le misure contrattuali sono tipicamente soggette a revisione e possono persino essere disattese dalle parti.

La probabilità di re-identificazione non è un dato statico. Essa tende ad aumentare nel tempo per effetto dei progressi nelle tecnologie e nelle tecniche impiegate, nonché della crescente disponibilità di informazioni aggiuntive. Qualora tale probabilità aumentasse fino a un livello non più trascurabile, i dati precedentemente anonimi dovrebbero essere nuovamente qualificati come personali, con conseguente responsabilità del titolare del trattamento per qualsiasi trattamento successivo. È pertanto buona prassi per i soggetti che elaborano dati anonimizzati rivalutare periodicamente, ove possibile e opportuno, la probabilità di re-identificazione.

Le Linee Guida sottolineano che l'anonimizzazione non è un'operazione neutra rispetto al regime del GDPR. I principi in materia di protezione dei dati trovano applicazione ogniqualvolta vengano trattati dati personali, ivi compresi i trattamenti finalizzati all'ottenimento di informazioni anonime. Ne discende, tra l'altro, che l'anonimizzazione deve fondarsi su un'idonea base giuridica ai sensi dell'art. 6 del GDPR e che, qualora il dataset contenga categorie particolari di dati personali, deve ricorrere una delle condizioni previste dall'art. 9, par. 2, del GDPR. Quanto alla trasparenza, i titolari del trattamento sono tenuti a rispettare i principi e gli obblighi informativi previsti dagli artt. 5, par. 1, lett. a), e 12-15 del GDPR anche con riferimento al processo di anonimizzazione. Devono, in particolare, dichiarare esplicitamente che i dati personali saranno trattati per produrre dati anonimi che esulano dall'ambito di applicazione del GDPR, evitando qualsiasi descrizione ambigua o fuorviante: ad esempio, non è lecito definire i dati "anonimi", "de-identificati" o "de-personalizzati" qualora gli interessati siano in realtà ancora identificabili. È inoltre necessario garantire un'adeguata documentazione del processo di anonimizzazione, ivi comprese le fasi di verifica degli insiemi di dati che si assumono anonimi, al fine di dimostrare sia la conformità al GDPR del processo stesso, sia l'effettività dell'anonimizzazione ottenuta.

Il quadro per la valutazione dell'anonimato sin qui descritto può essere applicato secondo due distinti approcci: quello contestuale, che tiene conto delle specifiche capacità e risorse del soggetto che riceve i dati e quello semplificato, che non differenzia i destinatari. L'approccio contestuale è più preciso, ma anche più complesso e può portare a errori se non si conoscono tutti i mezzi disponibili. D'altro canto, l'approccio semplificato non costituisce uno standard giuridico alternativo, trattando come personali dati che potrebbero in realtà non esserlo. I due approcci non si escludono a vicenda. In molti casi, una loro combinazione può rivelarsi più efficace, ad esempio, il titolare può avviare la valutazione con l'approccio semplificato, verificando se la re-identificazione sia teoricamente possibile: qualora non lo sia, i dati possono essere considerati anonimi. Se invece vengono individuati possibili metodi di re-identificazione, si passa all'approccio contestualizzato, verificando se tali metodi siano realisticamente e ragionevolmente utilizzabili dalle entità interessate. In alternativa, il titolare può avvalersi direttamente dell'approccio contestualizzato qualora, nella fase di mappatura dei dati, emerga la possibilità di escludere rapidamente i metodi di re-identificazione che non risultano applicabili in concreto. Superata la fase di mappatura, il test da condurre si articola sulla base di tre criteri, da verificare congiuntamente.

No Record Isolation

Il primo criterio riguarda l'assenza della possibilità di isolare un singolo individuo all'interno di un insieme di dati mediante uno o più attributi a esso riferibili. Il criterio è soddisfatto se i dati nel dataset non contengono una combinazione unica di attributi riconducibili a un singolo individuo. La probabilità di unicità aumenta, in particolare, quanto più numerosi e dettagliati sono gli attributi associati a ciascun record, tanto più elevata sarà la probabilità che risulti unico all'interno del dataset.

No Linkage

Il secondo criterio attiene all'impossibilità di stabilire collegamenti tra le informazioni contenute nel dataset e quelle presenti in altre banche dati. Il requisito è soddisfatto quando nessun record può essere associato, con certezza o con un elevato grado di probabilità, a un altro record

appartenente a un dataset differente e riferibile al medesimo individuo.

No Inference

Il terzo criterio riguarda la possibilità di ricavare, a partire dai dati disponibili, informazioni ulteriori e significative riferibili a uno specifico individuo. Il requisito è soddisfatto quando i dati non consentono di formulare deduzioni sufficientemente precise su una determinata persona. L'inferenza assume carattere specifico quando l'informazione dedotta può essere riferita a un individuo identificato o comunque identificabile. Essa è inoltre rilevante quando la deduzione deriva concretamente dai dati considerati, può incidere sui diritti o sugli interessi dell'interessato e non costituisce una semplice conclusione desumibile da conoscenze generali o da informazioni statistiche riferite alla popolazione nel suo complesso.

Se tutti e tre i criteri risultano soddisfatti, l'informazione può essere qualificata come anonima. Il mancato rispetto di uno o più criteri non implica tuttavia necessariamente che i dati debbano essere considerati personali: in tal caso, è necessario proseguire l'analisi per valutare l'impatto dei criteri insoddisfatti e verificare se i dati possano comunque essere considerati anonimi.

Nel caso in cui le tecniche di anonimizzazione non producessero risultati uniformi per tutti gli individui inclusi, e il dataset nel suo complesso contenga pertanto un insieme misto di dati personali e anonimi, l'intero dataset deve essere trattato come contenente dati personali, e quindi ricadente nell'ambito di applicazione del GDPR, in qualsiasi situazione in cui le diverse componenti non vengano trattate separatamente.

Le Linee Guida hanno così individuato diversi profili di rilevanza operativa per i titolari del trattamento chiamati a confrontarsi con le sfide sempre più complesse dell'anonimizzazione nell'era dell'intelligenza artificiale. Sul punto è infatti importante sottolineare che la maggior parte delle tecniche di re-identificazione attualmente documentate risulta di crescente accessibilità, richiede risorse limitate e può essere eseguita in tempi ragionevoli, persino su hardware di uso corrente, circostanza che l'EDPB ha segnalato come particolarmente significativa alla luce dei progressi nell'intelligenza artificiale, che potranno ulteriormente ridurre tempi e costi di accesso e impiego di tali tecniche.



Roberto A. Jacchia
PARTNER

r.jacchia@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano



Camillo Campli
ASSOCIATE

c.campli@dejalex.com
+39 06 809154.1
Via Vincenzo Bellini 24
00198 – Roma

Anna Chiara Frascari
TRAINEE LAWYER

a.frascari@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

MILANO
Via San Paolo, 7 · 20121 Milano, Italia
T. +39 02 72554.1 · F. +39 02 72554.400
milan@dejalex.com

ROMA
Via Vincenzo Bellini, 24 · 00198 Roma, Italia
T. +39 06 809154.1 · F. +39 06 809154.44
rome@dejalex.com

BRUXELLES
Chaussée de La Hulpe 187 · 1170 Bruxelles, Belgique
T. +32 (0)26455670 · F. +32 (0)27420138
brussels@dejalex.com

MOSCOW
Potapovsky Lane, 5, build. 2, 4th floor, office 401/12/9 · 101000, Moscow, Russia
T. +7 495 792 54 92 · F. +7 495 792 54 93
moscow@dejalex.com