I dati amministrativi: le regole del GDPR per l'uso a fini statistici e di ricerca

Chiara di Somma
Garante per la protezione dei dati personali

Il valore del patrimonio informativo delle pubbliche amministrazioni per fini statistici e di ricerca, ivi incluse analisi previsionali, è aumentato in maniera esponenziale con l'evoluzione delle tecniche di elaborazione e studio dei dati accrescendo proporzionalmente la sua funzione strategica per le c.d. *Evidence-Based Policy*. Buona parte delle banche dati amministrative sono popolate di dati di carattere personale, spesso anche particolarmente sensibili. Questa circostanza, lungi dal costituire un ostacolo al loro riutilizzo, impone purtuttavia il rispetto di specifiche regole e condizioni. Senza pretese di esaustività, il presente contributo intende offrire una panoramica degli aspetti rilevanti della normativa in materia di protezione dei dati personali trattati per il perseguimento degli scopi di statistica, in particolare nell'ambito del Sistema statistico nazionale.

Administrative data: GDPR rules for statistical and research use

The value of the information assets held by public administrations for statistical and research purposes – including predictive analysis – has increased exponentially alongside the evolution of data processing and analysis techniques, proportionally enhancing its strategic function for so-called Evidence-Based Policies. A significant portion of administrative databases is populated with personal data, often of a sensitive nature. This circumstance, far from constituting an obstacle to their reuse, nevertheless necessitates compliance with specific rules and conditions. Without claiming to be exhaustive, this contribution aims to provide an overview of the relevant aspects of the regulatory framework concerning the protection of personal data processed for statistical purposes, with particular reference to the National Statistical System.

DOI: 10.53223/Sinappsi_2026-02-1

Citazione
di Somma C. (2026), I dati amministrativi: le regole del GDPR per l'uso a fini statistici e di ricerca, *Sinappsi*, XVI, n.2, pp.24-33

Parole chiave
Dati amministrativi
Protezione dei dati personali
Statistica

Keywords
Administrative data
Data Protection
Statistics

1. Il trattamento dei dati amministrativi nel Sistema statistico nazionale: le origini

Il quadro normativo, che più di ogni altro testimonia il valore delle banche dati amministrative come fonte informativa per orientare il decisore pubblico nelle scelte programmatiche, è quello della statistica ufficiale; la scienza dello Stato che usa i suoi stessi dati per una migliore comprensione dell'andamento, degli sviluppi, delle necessità della società (di Somma 2022).

Con la legge 23 agosto 1988, n. 400, il Governo veniva delegato "ad emanare, [...], norme aventi valore di legge ordinaria per la riforma degli enti e degli organismi pubblici di informazione statistica in base ai seguenti principi e criteri direttivi: a) che sia attuato il sistematico collegamento e l'interconnessione di tutte le fonti pubbliche preposte alla raccolta e alla elaborazione dei dati statistici a livello centrale e locale; [...]; d) che sia garantito il principio dell'imparzialità e della completezza nella raccolta, nella elaborazione e nella diffusione dei dati; e) che sia garantito l'accesso diretto da parte del Parlamento, delle regioni, di enti pubblici, di organi dello Stato, di persone giuridiche,

di associazioni e singoli cittadini ai dati elaborati con i limiti espressamente previsti dalla legge e nel rispetto dei diritti fondamentali della persona [...]".

In attuazione della delega è stato adottato il decreto legislativo 6 settembre 1989, n. 322 recante *Norme sul Sistema Statistico Nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'art. 24 della legge 23 agosto 1988, n. 400*. Un testo organico relativo al funzionamento del Sistema statistico nazionale (di seguito Sistan), ancora pienamente vigente e che ha subito specifiche modifiche, in particolare per un progressivo adeguamento alla normativa in materia di protezione dei dati personali[1].

Il decreto prevede l'interconnessione e il collegamento dei sistemi informativi delle pubbliche amministrazioni con il Sistan, consentendo agli uffici di statistica l'accesso a tutti i dati in possesso dell'amministrazione di appartenenza (art. 6, commi 2 e 3). Introducendo il Programma statistico nazionale (di seguito PSN), ossia lo strumento normativo triennale (aggiornato annualmente) che pianifica le indagini e le rilevazioni statistiche di interesse pubblico, il D.Lgs. 322 del 1989 ha imposto l'obbligo a tutte le amministrazioni, enti e organismi pubblici, nonché ai privati – se previsto nel PSN – di fornire i dati loro richiesti per le rilevazioni ivi previste (art. 7).

A tutela dei dati trattati, l'art. 9 impone il segreto statistico e il c.d. divieto di ricadute amministrative[2], in base al quale i dati raccolti per scopi statistici non possono essere utilizzatati per altri fini. Il decreto prevede poi, all'art. 10, una norma di raccordo tra il Sistan e i ricercatori che operano al di fuori di esso[3] per favorire la circolazione di questo importante patrimonio informativo anche nel contesto scientifico.

Il D.Lgs. n. 322 del 1989, in origine, si limitava ad individuare il punto di equilibrio tra le esigenze di accesso e di utilizzo di dati, da un lato, e le misure per il corretto ed efficace svolgimento dell'attività statistica dall'altro, facendo leva in particolare sull'indipendenza della ricerca, sul segreto statistico, e, quindi sulla natura anonima e aggregata dei relativi output. Le successive modifiche hanno integrato questo delicato equilibrio con norme volte ad armonizzare la disciplina statistica con quella in materia di protezione dei dati personali, facendo, peraltro, emergere all'atto pratico una massima convergenza tra i principi sui quali si fondano le due differenti discipline, come si avrà modo di illustrare nel prosieguo.

Determinante, infine, la più volte novellata previsione (di cui all'art. 6-bis del D.Lgs. n. 322 del 1989) relativa alle condizioni di liceità del trattamento dei dati personali ivi inclusi quelli c.d. sensibili svolti dai soggetti Sistan, in particolare, per la realizzazione delle rilevazioni previste nel PSN, la cui adozione richiede il preventivo parere del Garante per la protezione dei dati personali (di seguito anche solo Garante per la privacy o Autorità)[4].

1 A seguito dell'entrata in vigore della legge n. 675 del 31 dicembre 1996 – *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, una prima modifica al D.Lgs. 322 del 1989 è stata apportata dal decreto legislativo 30 luglio 1999, n. 281, recante *Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica*. Più di recente, il decreto-legge 28 gennaio 2019, n. 4 convertito con modificazioni dalla legge 28 marzo 2019, n. 26, ha novellato il D.Lgs. 322 del 1989 per armonizzarlo con il *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 Regolamento generale sulla protezione dei dati* (GDPR) nonché con il *Codice in materia di protezione dei dati personali,* D.Lgs. 30 giugno 2003, così come modificato dal D.Lgs. 10 agosto 2018, n. 101 (Codice della privacy).

2 L'art. 9 del D.Lgs. 322 del 1989 dispone che "I dati raccolti nell'ambito di rilevazioni statistiche comprese nel programma statistico nazionale da parte degli uffici di statistica non possono essere esternati se non in forma aggregata, in modo che non se ne possa trarre alcun riferimento relativamente a persone identificabili, e possono essere utilizzati solo per scopi statistici".

3 Cfr. art. 10 rubricato *Accesso ai dati statistici* del D.Lgs. 322 del 1989 e *infra* par. 5.

4 L'art. 6-bis (commi 1 e 1-*bis*) del D.Lgs. 322 del 1989 che dispone "1. I soggetti che fanno parte o partecipano al Sistema statistico nazionale possono raccogliere ed ulteriormente trattare i dati personali necessari per perseguire gli scopi statistici previsti dal presente decreto, dalla legge o dalla normativa comunitaria, qualora il trattamento di dati anonimi non permetta di raggiungere i medesimi scopi. 1-bis. Per i trattamenti di dati personali, compresi quelli di cui all'articolo 9 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, effettuati per fini statistici di interesse pubblico rilevante ai sensi dell'articolo 2-*sexies*, comma 2, lettera cc), del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, in conformità all'articolo 108 del medesimo Codice, nel Programma statistico nazionale sono specificati i tipi di dati, le operazioni eseguibili e le misure adottate per tutelare i diritti fondamentali e le libertà degli interessati, qualora non siano individuati da una disposizione di legge o di regolamento. Il Programma statistico nazionale, adottato sentito il Garante per la protezione dei dati personali, indica le misure tecniche e organizzative idonee a garantire la liceità e la correttezza del trattamento, con particolare riguardo al principio di minimizzazione dei dati, e, per ciascun trattamento, le modalità, le categorie dei soggetti interessati, le finalità perseguite, le fonti utilizzate, le principali variabili acquisite, i tempi di conservazione e le categorie dei soggetti destinatari dei dati. Per i trattamenti dei dati personali di cui all'articolo 10 del citato regolamento (UE) 2016/679 effettuati per fini statistici di interesse pubblico rilevante ai sensi del citato articolo 2-sexies, comma 2, lettera cc), del codice di cui al decreto legislativo n. 196 del 2003 trova applicazione l'articolo 2-*octies* del medesimo codice) [...]". Per i trattamenti di dati personali relativi a condanne penali e reati, la normativa in esame rinvia quindi all'articolo 2-*octies* del Codice della privacy che in assenza di una specifica norma di legge o di regolamento, rinvia a sua volta ad un decreto del Ministero della Giustizia, ai sensi dell'art. 17, comma 3 della legge 23 agosto 1988, n. 400. Il Garante per la privacy, con il provvedimento n. 247 del 24 giugno 2021 (doc. web n. 9682603), ha espresso il parere su uno Schema di regolamento recante l'individuazione dei trattamenti di dati personali relativi a condanne penali e reati e delle relative garanzie appropriate, ai sensi dell'articolo 2-*octies*, comma 2 del Codice della privacy.

Ciò ha consentito la produzione di una copiosa giurisprudenza da parte dell'Autorità, che ha contribuito nel corso del tempo a definire il rapporto tra statistica e protezione dei dati personali, attraverso l'indicazione di specifici accorgimenti e misure per l'uso dei dati di carattere personale, anche inerenti alle particolari categorie, contenuti in banche date pubbliche (che qui definiamo 'dati amministrativi'), tenendo anche conto dell'evoluzione, da un canto, del processo tecnologico e, dell'altro, della scienza statistica stessa[5] (Longo 2017; Ponti 2023; Simonati 2023).

Tutto ciò premesso, si intende ora passare all'esame dei tratti del Regolamento generale sulla protezione dei dati, Regolamento (UE) 2016/679 (di seguito Regolamento o GDPR) e del Codice in materia di protezione dei dati personali, D.Lgs. 30 giugno 2003 (di seguito Codice della privacy) più rilevanti per il trattamento dei dati amministrativi a fini statistici, per poi soffermarsi sulle misure più adeguate per un equo bilanciamento tra protezione dei dati personali e attività statistica.

2. La statistica nel GDPR

Il Regolamento disciplina particolarmente il trattamento dei dati personali per finalità statistiche, dimostrando una sorta di '*favor*'[6] del Legislatore comunitario per tale scopo.

Esso, infatti, introduce nel settore in esame: una deroga ai principi di limitazione della finalità e della conservazione (art. 5, par. 1, lett. b) e e) GDPR)[7]; una specifica esenzione al divieto di trattare le particolari categorie di dati, (art. 9, par. 1 e 2, lett. j) GDPR); deroghe e limitazioni ai diritti spettanti agli interessati in relazione ai loro dati personali (artt. 14, par. 5 lett. b), 17, par. 2 lett. d), 21, par. 6, 89, par. 2). Infine, il capo IX, concernente le specifiche situazioni di trattamento, all'art. 89, rubricato *Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*, impone l'applicazione di garanzie adeguate per i diritti e le libertà dell'interessato, facendo esplicito riferimento alla pseudonimizzazione dei dati.

Nella dimensione nazionale, in attuazione dell'art. 89 del GDPR, il Codice della privacy affida, in particolare al titolo VII – parte II (artt. da 97 a 110-bis), la disciplina dei trattamenti di dati personali a fini di ricerca scientifica e statistici introducendo: regole di carattere generale (artt. 97 e 99); un coacervo di norme dedicate alla ricerca scientifica e statistica (artt. 104-107 e 110-bis); una disciplina specifica per il trattamento di dati personali per scopi di statistica da parte dei soggetti Sistan (artt. 108-109).

In tale quadro, merita rilievo l'art. 105 del Codice della privacy che ribadisce che gli scopi di ricerca scientifica e statistici si presumono non incompatibili con quello della raccolta, qualunque essi siano, precisando che, viceversa, nessuno scopo ulteriore differente è ammesso per i dati raccolti per scopi di ricerca scientifica. Si tratta del c.d. "divieto di ricadute amministrative", elemento cardine anche dei principi internazionali ed europei per l'uso a fini statistici dei dati personali, secondo cui "dovrebbe essere severamente proibito" l'uso di dati raccolti a fini statistici per altri scopi, ad esempio "amministrativi, giuridici o fiscali", oppure per "condurre verifiche nei confronti delle unità statistiche"[8].

5 *Ex multis* si vedano i provvedimenti n. 315 del 16 settembre 2021 (doc. web n. 9717477); n. 434 del 16 dicembre 2021 (doc. web n. 9738899); n. 237 del 30 giugno 2022 (doc. web n. 9794929).

6 Sul punto occorre precisare come tale '*favor*' non possa considerarsi frutto di una decisione arbitraria ma della precisa consapevolezza che l'attività statistica – espressione di un diritto costituzionalmente tutelato (artt. 9 e 33 della Costituzione) – necessita di regole precipue per un equo bilanciamento con il diritto alla protezione dei dati personali, che al contempo non la renda inefficace o ne ostacoli indebitamente l'esercizio.

7 Merita segnalarsi in particolare che in base al "principio di limitazione della finalità", i dati sono "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali" e, che, in base al "principio di limitazione della conservazione", i dati sono "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato" (art. 5, par. 1, lett. b) e) GDPR; cfr. anche art. 99 del Codice della privacy) cfr. Gruppo articolo 29, *Opinion 03/2013 on purpose limitation,* del 2 aprile 2013; Provv. del Garante per la privacy del n 406 del 1° novembre 2021 (doc. web n. 9731827).

8 Cfr. il Considerando n. 27 del Regolamento CE N. 2009/223 sulle statistiche europee e, a livello internazionale, l'art. 4 della Raccomandazione del Consiglio d'Europa n. R (97) relativa alla protezione dei personali raccolti e trattati per scopi statistici. Il Garante per la privacy si è espresso numerosissime volte in riferimento a questo principio: cfr. *ex multis*: Provv. 271 del 9 maggio 2018 n. (doc. web n. 9001732); n. 270 del 17 dicembre 2020 (doc. web n. 9523274); n. 10 del 23 gennaio 2020 (doc. web. n. 9261093); n. 434 del 16 dicembre 2021 (doc. web n. 9738899).

3. Le condizioni di liceità del trattamento

La raccolta e il successivo trattamento di dati amministrativi per fini statistici da parte dei soggetti che fanno parte o partecipano al Sistan sono ammessi alle condizioni di cui all'art. 6, par. 1, lett. c) ed e) parr. 2 e 3 del Regolamento[9]. Qualora il trattamento sia destinato a coinvolgere dati c.d. 'sensibili', rileva invece la deroga al divieto dell'uso di tali informazioni, di cui alla lett. g), del par. 2, dell'art. 9 del GDPR (Bombardelli 2022; Califano 2017; Caravà 2019; Carullo 2024; Franca 2023; Francario 2022; Garofoli e Ferrari 2008).

In attuazione dell'art. 6, par. 3 del Regolamento, l'art. 2-quater del Codice della privacy ha conferito all'Autorità il compito di promuovere, nell'osservanza del principio di rappresentatività, l'adozione di regole deontologiche per i trattamenti previsti, tra agli altri, al capo IX del Regolamento (Bifulco 2021).

Rilevano quindi le *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale*, corrispondenti all'allegato A4 al Codice della privacy, che costituiscono condizione essenziale di liceità e correttezza del trattamento, nella misura in cui la loro violazione può comportare l'applicazione di una sanzione amministrativa, ai sensi dell'art. 166 del Codice della privacy[10].

4. L'art. 89, par. 1 del Regolamento e le garanzie adeguate per i diritti e le libertà dell'interessato

Quanto fin ora rappresentato dimostra come il Regolamento e per esso, laddove necessario (Baroncelli 2008), l'ordinamento nazionale, individuino ampie possibilità per l'uso dei dati amministrativi a fini statistici, fornendo un sistema di regole articolato e complesso che non si esaurisce in formali previsioni normative ma che richiede anzi obbligatoriamente altresì l'implementazione di misure adeguate sia alla tutela dei diritti e delle libertà fondamentali degli interessati sia a garantire il rispetto degli obblighi derivanti dal Regolamento. Ci si riferisce in particolare al già citato art. 89 del Regolamento[11].

Si tratta di una norma cogente che, lungi dall'avere un valore meramente indicativo, è accompagnata di uno specifico presidio sanzionatorio. L'art. 83, par. 5, lett. d) del GDPR, infatti, dispone l'applicazione di una sanzione amministrativa per la violazione di "qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX" (nell'ordinamento interno gli artt. 97 e ss. del Codice della privacy).

L'art. 89 da una parte esorta, dall'altra sembra proprio imporre l'uso di misure di pseudonimizzazione ossia di quel trattamento a seguito del quale "i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4, n. 5 GDPR). In altri termini, la pseudonimizzazione sostituisce parte dei dati con uno o più codici pseudonimi[12] (Basdekis *et al.* 2023).

La reversibilità dei codici pseudonimi (che determina la natura identificativa del dato pseudonimizzato, *Cons.* 26 GDPR) è assicurata da informazioni aggiuntive, il cui trattamento richiede quindi (al pari dei dati personali) l'implementazione di specifiche misure tecniche e organizzative adeguate a garantirne la sicurezza,

9 Nell'ordinamento interno le disposizioni di cui agli artt. 6, par.1, lett. c) e e) e art. 9, par. 2, lett. g) del GDPR hanno trovato ulteriore specificazione, rispettivamente, negli artt. 2- *ter* e 2-*sexies* del Codice della privacy, secondo i quali la base giuridica del trattamento deve risiedere in una norma dell'Unione o in una norma di legge, regolamento o atto amministrativo generale dell'ordinamento interno (tra queste quindi il PSN); sono inoltre richieste ulteriori garanzie per i dati c.d. sensibili (art. 9 GDPR). Cfr. Garante europeo per la protezione dei dati (di seguito EDPS) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit,* 11 aprile 2017*; Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data,* 19 dicembre 2019*; Guidance for co-legislators on key elements of legislative Proposals,* 7 maggio 2025).

10 Si segnalano altresì le *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica*, di cui all'allegato A5 del Codice. Con il provvedimento n. 133 del 15 aprile 2021 (doc. web n. 9582086). L'Autorità ha adottato la deliberazione di promovimento delle nuove *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale*, n. 98 doc. web n. 9107633 e con provvedimento n. 298 del 4 maggio 2024 (doc. web n. 10016146) la deliberazione di promovimento delle *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica* ai sensi degli artt. 2-quater e 106 del Codice.

11 Cfr. EDPS (European Data Protection Supervisor), *Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research*, *Final Report* dell' 8 febbraio 2019.

12 Cfr. Comitato europeo per la protezione dei dati (EBPB) *Guidelines 01/2025 on Pseudonymisation Adottate il 16 Gennaio 2025*; Garante per la privacy, Provvedimenti n. 10 del 23 gennaio 2020 (doc. web 9261093); n. 315, 16 settembre 2021 (doc. web n. 9717477); n. 674 del 13 novembre 2024, (doc. web n. 10090499).

tra le quali, in primo luogo, la segregazione rispetto alle informazioni pseudonimizzate[13].

La pseudonimizzazione va intesa, non solo, come una misura per ridurre i rischi correlati al trattamento dei dati personali (es. violazione della riservatezza, alterazione dei dati, *function creep*) ma è anche, laddove sapientemente impiegata congiuntamente ad altre misure tecniche e organizzative, quale utile strumento per il rispetto degli obblighi di protezione dei dati personali in generale (es. effettiva applicazione dei principi di liceità, limitazione della finalità, minimizzazione dei dati, limitazione della conservazione, obblighi di *privacy by design* e *by default*[14] misure per il trasferimento dei dati all'estero o a soggetti terzi, cfr. *Cons.* 28 GDPR). Non sarebbe, quindi, corretto fare affidamento, per l'applicazione dei principi del Regolamento e in particolare di quello di integrità e riservatezza di cui all'art. 5, par. 1 lett. f), sulla sola pseudonimizzazione dei dati, vieppiù in caso di trattamento delle particolari categorie (Stalla-Bourdillon 2025).

Si comprende tuttavia, in termini generali, la particolare adeguatezza di questa misura nel contesto della statistica. Tale scienza, infatti, è volta ad analizzare, investigare e studiare fenomeni collettivi, la loro evoluzione, la loro incidenza, le loro cause, ma è per sua natura scarsamente interessata all'identità dei singoli soggetti coinvolti in tali fenomeni. Sono piuttosto gli attributi dei singoli, spesso anche (doverosamente) generalizzati, gli elementi (*rectius* i dati) di interesse della statistica. In linea generale, infatti, pur necessitandosi di informazioni relative ad un singolo individuo, risulta eccedente e sproporzionato il trattamento anche di quelle che ne consentono l'identificazione diretta. Ciò ferma restando la possibilità di risalire all'identità del singolo laddove necessario (ad esempio a fini di monitoraggio o controlli di qualità e di copertura); possibilità che la pseudonimizzazione dei dati fa salva.

Occorre considerare, inoltre, come l'attività statistica si sia evoluta nel corso del tempo, passando da un sistema incentrato prevalentemente sulle rilevazioni dirette a uno che predilige la statistica c.d. da fonti amministrative organizzate[15]. In altri termini, buona parte delle statistiche pubbliche, ivi inclusa l'attività censuaria[16], si basa in misura sempre più preponderante sull'interconnessione, lo studio e lo svolgimento di analisi previsionali su dati amministrativi.

Gli enti Sistan utilizzano per i propri scopi molteplici fonti amministrative, riducendo così il c.d. 'fastidio statistico', tipico delle rilevazioni dirette e i costi connessi a tali operazioni, e migliorando la qualità dei dati trattati. I soggetti Sistan – e tra questi in particolare l'Istituto nazionale di statistica - Istat o gli uffici di statistica delle grandi pubbliche amministrazioni – quindi, detengono ed elaborano ulteriormente enormi quantità di dati, spesso anche sensibili, venendosi a determinare un trattamento su larga scala e ad alto rischio[17]. Si tratta di un patrimonio informativo inestimabile per la statistica, ma al tempo stesso di una fonte di elevato rischio per i diritti e le libertà fondamentali degli interessati, che richiede l'impiego di specifiche misure tecniche e organizzative di mitigazione e contenimento[18].

La pseudonimizzazione è una di queste, con l'ulteriore vantaggio che essa, nel contribuire ad assicurare il rispetto del GDPR, può operare anche a beneficio della stessa attività statistica. A titolo meramente esemplificativo è intuitivo osservare come, garantendo la riservatezza del dato, si assicuri altresì una migliore attuazione del segreto statistico o come i principi di minimizzazione ed esattezza dei dati possano altresì contribuire ad accrescere la qualità del campione statistico[19].

13 Le informazioni pseudonimizzate vengono in questo modo a costituire un 'dominio' autonomo cfr. punto 2.3 delle *Guidelines 01/2025 on Pseudonymisation* cit. e provvedimento dell'Autorità n. 10 del 23 gennaio 2020, cit.

14 Provvedimento del Garante per la privacy n. 10 del 23 gennaio 2020, cit.

15 Le statistiche da indagine (SDI) presuppongono un contatto diretto con l'interessato e, dunque, non solo la possibilità per quest'ultimo di non fornire riscontro alle domande relative ai dati sensibili o giudiziari (che sono esenti dal c.d. obbligo di risposta ai sensi dell'art. 7, comma 2, D.Lgs. n. 322/1989) ma anche che siano resi riscontri inesatti o approssimativi. Per contro, nelle statistiche da fonti amministrative organizzate (SDA) l'ente Sistan, titolare del lavoro statistico – in virtù del PSN, che funge da base giuridica del trattamento – può raccogliere dati personali, anche inerenti alle particolari categorie presumibilmente più accurati, presso altri soggetti pubblici o privati che sono tenuti a formili.

16 Cfr. art. 1, commi 227, 228, 232 della legge 27 dicembre 2017, n. 205 recante *Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020*.

17 Cfr. art. 35 GDPR e Gruppo art. 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato"* ai fini del Regolamento (UE) 2016/679 adottate 4 ottobre 2017.

18 Si segnala al riguardo il Provvedimento n. 46 del 10 febbraio 2022 (doc. web n. 9751194), relativo a un *data breach* occorso ad alcuni database dell'Istat.

19 EDPS, *Guidance for Risk Management of Artificial Intelligence systems* dell'11 novembre 2025.

Assistiamo quindi ad un singolare caso in cui l'operazione di bilanciamento, necessaria per la coesistenza di attività espressione di diritti giuridicamente tutelati, piuttosto che comprimerli (facendo leva solo sulla loro naturale elasticità) ne amplifica la piena estrinsecazione. Un bilanciamento che non opera, quindi, nel 'conflitto di diritti' ma per aumentarne la convergenza.

L'art. 89 del GDPR auspica infine che il perseguimento dei fini ulteriori di statista avvenga, laddove possibile, attraverso misure che non consentano più di identificare gli interessati. Costituisce, invero, una precondizione di tutto l'impianto della normativa in materia di protezione dei dati personali l'assunto che questi vadano trattati solo se necessari[20], dovendosi, laddove possibile, preferire informazioni non personali o anonimizzate. Ciononostante le differenti tecniche di anonimizzazione[21], indispensabili in fase di diffusione dei risultati statistici, solitamente diminuiscono, dall'ottica del ricercatore, il potenziale informativo del dato, specie se comportano la perdita di granularità della informazione.

L'approccio responsabile e proattivo richiesto dal GDPR, in virtù dei principi di *accountability* e di *privacy by design* e *by default* (artt. 5, par. 2 e 25), impone tuttavia al titolare di esplorare l'utilità di talune nuove tecnologie capaci di offrire soluzioni coerenti con lo stato dell'arte tecnologica, adatte anche a valorizzare l'uso dei dati anonimizzati, ciò in particolare quando oggetto di trattamenti sono dati di natura "sensibile" (D'Acquisto e Naldi 2017).

Ci si riferisce alle c.d. *Privacy-enhancing technologies* (PET) e tra queste, in particolare, alla tecnica della sintetizzazione dei dati che offre una concreta alternativa all'uso di dati di carattere personale. Quelli sintetici, infatti, sono dati creati da strumenti di intelligenza artificiale che, partendo da dati reali, forniscono informazioni ad esse analoghe e con lo stesso valore informativo ma non identificative degli interessati (Aceto *et al.* 2024; Bassan *et al.* 2018; Boudewijn *et al.* 2023; Brusadelli *et al.* 2025; Carr *et al.* 2023; Chenna 2022; D'Acquisto 2024; El Emam *et al.* 2020). Come anticipato, la pseudonimizzazione e l'anonimizzazione sono operazioni di trattamento che incidono in maniera sostanzialmente differente sui dati personali: la prima assicurando la possibilità di risalire all'interessato, la seconda negandola.

L'anonimizzazione costituisce la *condicio sine qua non* per la diffusione dei risultati statistici e per la tutela del segreto posta a garanzia delle informazioni trattate a tale fine.

Merita brevemente quindi richiamare un importante e recente arresto della Corte di Giustizia dell'Unione europea, la sentenza del 4 settembre 2025, C-413/23, che, partendo dalle indicazioni contenute nel *Considerando* 26 del GDPR[22] ha accorciato le distanze tra tali operazioni di trattamento, esplorando la possibilità che, in determinati contesti, informazioni oggetto 'solo' di pseudonimizzazione possano comunque perdere la capacità di reindentificare gli interessati ai quali si riferiscono. Ebbene, la Corte è giunta a sostenere che in alcune circostanze, la pseudonimizzazione possa di fatto incidere sul carattere personale dei dati, a condizione che le informazioni aggiuntive siano conservate separatamente e vengano attuate misure tecniche

20 EDPS, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, cit.

21 Il dato anonimizzato, al quale non si applica la disciplina in materia di protezione dei dati personali, è tale solo se non consente l'identificazione diretta o indiretta di una persona, tenuto conto di tutti i mezzi ragionevoli (informazioni, risorse tecnologiche ed economiche, competenze, tempo) nella disponibilità di chi (titolare o altro soggetto) provi a identificare un interessato. L'anonimizzazione, deve pertanto impedire che si possa: 1. isolare una persona in un gruppo (*single-out*); 2. collegare un dato anonimizzato a dati riferibili a una persona presente in un distinto insieme di dati (*linkability*); 3. dedurre nuove informazioni riferibili a una persona da un dato anonimizzato (*inference*). Gruppo art. 29 *Parere 05/2014 sulle tecniche di anonimizzazione*, adottato il 10 aprile 2014.

22 Il *Considerando* 26 del GDPR stabilisce che "È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. 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. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. 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 l'identificazione dell'interessato. Il presente Regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca".

e organizzative tali da garantire in modo effettivo che i dati pseudonimizzati non siano attribuiti a una persona fisica identificata o identificabile. In altri termini, la natura identificativa dei dati pseudonimizzati dovrebbe, a mente della Corte, cessare di essere un assioma ma dipendere da una valutazione in concreto, condizionata dal contesto nel quale essi approdano e della sussistenza di mezzi che ragionevolmente possano favorire la reindentificazione degli interessati (*Cons.* 26 GDPR) (Bird&Bird 2025; He 2023; Lee 2025; Yermilov *et al.* 2023).

Ci si dovrà quindi interrogare sull'impatto di tale rinnovata interpretazione di dato pseudonimizzato e anonimizzato nell'attività statistica, specie qualora la modifica alla definizione di dato personale proposta dalla Commissione europea di Regolamento della c.d. *digital omnibus* dovesse trovare attuazione[23]. Azzardando una previsione, si ritiene che tale evoluzione potrebbe, anzi dovrebbe, avere un impatto pressoché nullo nel rigore delle valutazioni sul rischio di reindetificazioni degli interessati in fase di diffusione dei risultati statistici. Ciò, non solo per la contestuale vigenza del segreto statistico, non derogabile, ma anche per l'imprevedibilità ex ante del rischio di reidentificazione degli interessati negli innumerevoli e differenti contesti dove gli output della statistica verranno ad essere trattati a seguito della loro diffusione.

5. Dalla statistica ufficiale alla ricerca

L'uso dei 'dati amministrativi' non è appannaggio esclusivo dei soggetti Sistan. Esistono, infatti, svariati strumenti normativi affinché di tale prezioso patrimonio informativo possano godere anche i ricercatori che operano al di fuori di tale contesto, sempre ferma l'applicazione di adeguate misure (Brizzi 2021; Stefanelli 2018).

Si richiama, quindi, l'art. 10 del D.Lgs. 322 del 1989, rubricato *Accesso ai dati statistici*, che dispone che: "*1.* I dati elaborati nell'ambito delle rilevazioni statistiche comprese nel programma statistico nazionale sono patrimonio della collettività e vengono distribuiti per fini di studio e di ricerca a coloro che li richiedono secondo la disciplina del presente decreto, fermi restando i divieti di cui all'art. 9. *2.* Sono distribuite altresì, ove disponibili, su richiesta motivata e previa autorizzazione del Presidente dell'Istat, collezioni campionarie di dati elementari, resi anonimi e privi di ogni riferimento che ne permetta il collegamento con singole persone fisiche e giuridiche […]".

Al riguardo, si segnala altresì dall´art. 5-ter del decreto legislativo del 14 marzo 2013, n. 33, rubricato *Accesso per fini scientifici ai dati elementari raccolti per finalità statistiche*, in base al quale gli enti e uffici del Sistan possano consentire l´accesso, per fini scientifici, ai dati elementari, privi di ogni riferimento che permetta l´identificazione diretta delle unità statistiche, raccolti nell´ambito di trattamenti statistici di cui i medesimi soggetti siano titolari, nel rispetto di una serie di condizioni. In particolare, vengono definiti: i requisiti per l´ente di ricerca di appartenenza dei ricercatori, per il progetto di ricerca e per le cui finalità vengono richiesti i dati, le modalità di rilascio dei dati, nonché le operazioni di trattamento eseguibili, facendo divieto di effettuare trattamenti diversi da quelli previsti nel progetto di ricerca, conservare i dati elementari oltre i termini di durata del progetto, comunicare i dati a terzi e diffonderli, pena l´applicazione della sanzione di cui all´art. 162, comma 2-*bis*, del Codice della privacy.

In attuazione di tale norma, il Comitato di indirizzo e coordinamento dell'informazione statistica (Comstat), sentito il Garante per la privacy[24], ha adottato la Direttiva n. 11 del 7 novembre 2018 recante *Linee guida per l'accesso a fini scientifici ai dati elementari del Sistan*. Esse, nel disciplinare in concreto tale flusso di dati, ne assicurano la protezione, prescrivendo specifiche misure per garantirne la sicurezza e affinché i risultati della ricerca non permettano il collegamento con le unità statistiche (Patti 2019).

Merita, infine, soffermarsi sull'art. 2-ter, comma 3 del Codice privacy che consente la comunicazione di dati 'comuni' tra soggetti che trattano dati per il perseguimento di un compito di interesse pubblico (si pensi ad esempio alle università) anche laddove tale flusso non sia previsto da una norma di legge, regolamento o atto amministrativo generale a condizione che ne sia data previa notizia al Garante per la privacy almeno 10 giorni prima dell'inizio dei trattamenti (di Somma 2019).

L'ordinamento italiano dispone poi di uno specifico corpo normativo sui c.d. sistemi di sorveglianza e registri di patologia, che detta le condizioni per il trattamento dei dati sulla salute ivi raccolti anche per fini di ricerca epidemiologica, la scienza biomedica che studia la frequenza, la distribuzione e le cause di eventi legati alla salute

23 EDPB-EDPS, *Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)* del 10 febbraio 2026.

24 L'Autorità si è espressa con il Parere del 21 giugno 2018 n. 388 (doc. web 9023239).

all'interno di una popolazione e che insieme alla statistica sanitaria costituisce la base scientifica della sanità pubblica (art. 12, commi da 10 a 14 del D.L. 18 ottobre 2012, n. 179 e ss.ii.mm; D.P.C.M. 3 marzo 2017, *Cons*. 157 GDPR).

Merita in conclusione oltrepassare i confini dell'ordinamento nazionale per segnalare la grande opportunità fornita al c.d. 'uso secondario' dei dati (che include quelli statistici e di ricerca) dal Regolamento europeo n. 327 del 2025, che ha istituito lo Spazio europeo dei dati sanitari (European Health Data Space, EHDS).

Nel Regolamento EHDS, per uso secondario dei dati si intende "il trattamento dei dati sanitari elettronici per le finalità indicate al capo IV del presente Regolamento, che sono diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti" (art. 2, par. 1, lett. e).

Tre le finalità (secondarie) per le quali è possibile trattare i dati sanitari elettronici, rilevano quelle "statistiche quali definite all'articolo 3, punto 1), del Regolamento (UE) n. 223/2009, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza" (art. 53, par. 1, lett. c) e quelle di "ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale (art. 53, par. 1, lett. e)".

Lo EHDS si inserisce perfettamente nelle maglie del GDRP nella misura in cui nell'indicare gli scopi secondari del trattamento (tra gli altri, lo si ribadisce, quello statistico e di ricerca) di determinate particolari categorie di dati e nel fornire, quindi, una solida base normativa (in attuazione degli artt. 5, par. 1 lett. a), 6 e 9 del GDPR), indica altresì le modalità con le quali concretamente i trattamenti necessari devono avere luogo, richiedendo, in particolare, la preventiva pseudonimizzazione o anonimizzazione dei dati (art. 89 GDPR e 55 e ss. EDHS) (Corso 2025; Foà 2026; Trubiani 2025)

Conclusioni

In conclusione, si è inteso in questa sede brevemente evidenziare come la centralità dei dati amministrativi per le attività di statistica e di ricerca trovi ampio riscontro in un quadro normativo nutrito, composito e articolato volto non a ostacolare il fine, ma anzi a sostenerlo, armonizzandolo al contempo con la normativa in materia di protezione dei dati personali.

Ciò non si esaurisce però con la formale osservanza delle norme, richiedendosi specifici e talvolta ingenti investimenti per l'individuazione e il costante aggiornamento di adeguate misure tecniche e organizzative e tra queste in particolare quella pseudonomizzazione dei dati[25].

Bibliografia

Aceto G., Giampaolo F., Guida C., Izzo S., Pescapè A., Piccialli F., Prezioso E. (2024), Synthetic and Privacy-Preserving Traffic Trace Generation using Generative AI Models for Training Network Intrusion Detection Systems, *Journal of Network and Computer Applications*, 229, art.103926, pp.1-16

Baroncelli S. (2008), Le fonti del diritto nell'UE dal Trattato di Roma al Trattato di Lisbona: verso un'accresciuta complessità del sistema, *Osservatoriosullefonti.it*, n.3, pp.1-46

25 Questo arresto giurisprudenziale è stato tenuto in considerazione dalla Commissione europea nella Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica i Regolamenti (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e le Direttive 2002/58/ce, (UE) 2022/2555 e (UE) 2022/2557 per quanto riguarda la semplificazione del quadro legislativo nel settore digitale e che abroga i Regolamenti (UE) 2018/1807, (UE) 2019/1150 e (UE) 2022/868 e la Direttiva (UE) 2019/1024 (*omnibus digitale*), del 19 novembre 2025. La proposta suggerisce infatti di modificare la definizione di dato personale contenuta del GDPR, con l'aggiunta all'art, 4, n. 1 del seguente capoverso "le informazioni relative a una persona fisica non sono necessariamente dati personali per qualsiasi altra persona o entità per il solo fatto che un'altra entità può identificare tale persona fisica. Le informazioni non sono personali per una determinata entità se quest'ultima non è in grado di identificare la persona fisica cui si riferiscono le informazioni, tenendo conto dei mezzi di cui tale entità si può ragionevolmente avvalere. Tali informazioni non diventano personali per tale entità per il solo fatto che un potenziale destinatario successivo dispone di mezzi di cui si può ragionevolmente avvalere per identificare la persona fisica cui le informazioni si riferiscono".

Basdekis I., Kloukinas C., Agostinho C., Vezakis I., Pimenta A., Gallo L. Spanoudakis G. (2023), Pseudonymisation in the context of GDPR-compliant medical research, in *19th International Conference on the Design of Reliable Communication Networks (DRCN)*, Vilanova i la Geltru, Spain, 2023, pp.1-6 <DOI:10.1109/DRCN57075.2023.10108370>

Bassan S., Harel O. (2018), The Ethics in Synthetics: Statistics in the Service of Ethics and Law in Health-Related Research in Big Data from Multiple Sources, *Journal of Law and Health*, 31, n.1, pp.87-110

Bifulco R. (2021), Codici di condotta e regole deontologiche dopo il D.Lgs. n. 101/2018, in Pizzetti F. (a cura di), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, Giappichelli, pp.337-350

Bird&Bird (2025), *Pseudonimizzazione e dati personali. Perché la sentenza CGUE 4 settembre2025, C-413/23 P potrebbe rappresentare un punto di svolta?,* London, Bird&Bird LLP

Bombardelli M. (2022), Dati personali (tutela dei), in Mattarella B.G., Ramajoli M. (a cura di), *Enciclopedia del diritto: i tematici*, Milano, Giuffrè, pp.351-381

Boudewijn A.T.P., Ferraris A.F., Panfilo D., Cocca V. (2023), *Privacy Measurements in Tabular Synthetic Data: State of the Art and Future Research Directions* <https://arxiv.org/abs/2311.17453>

Brizzi D. (2021), *Dati sanitari, GDPR, e Covid-19. Il caso della ricerca: tra scienza e diritto*, Milano, Giuffrè Francis Lefebvre

Brusadelli A., Ruffo D., di Somma C., Boudewijn A.T.P (2025), Ripensare l'evidenza: approccio multidisiciplinare all'uso dei dati sintetici in ambito sanitario - Parte I, *BioLaw Journal-Rivista di BioDiritto,* n.3, pp.317-340

Califano L. (2017), Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dati personali, in Califano L., Colapietro C. (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale Scientifica, pp.17-44

Caravà E. (2019), Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, in Sciaudone R., Caravà E. (a cura di), *Codice della privacy*, Pisa, Pacini Giuridica, pp.45-54.

Carr M., Wiemers E., Pollak A., McCue K. (2023), Using Synthetic Data to Estimate Earnings Dynamics Evidence from the SIPP GSF and SIPP SSB, *SSRN Electronic Journal*, pp.1-55

<DOI:10.2139/ssrn.4480922>

Carullo G. (2024), Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy, *Ceridap. Rivista interdisciplinare sul diritto delle amministrazioni pubbliche,* n.3, pp.37-52

Chenna S. (2022), *Application of Generative Adversarial Networks (GANs) for Generating Synthetic Data and in Cybersecurity*, *SSRN Electronic Journal*, pp.1-6 <DOI:10.2139/ssrn.4305711>

Corso S. (2025), *Autodeterminazione e dati sanitari*, Torino, Giappichelli

D'Acquisto G. (2024), Synthetic data and data protection laws*, Journal of data protection & Privacy*, 6, pp.227-236

D'Acquisto G., Naldi M. (2017), *Big data e Privacy by design*, Torino, Giappichelli

di Somma C. (2022), Ricerca scientifica storica e per finalità statistiche, in Riccio G.M., Scorza G., Belisario E. (a cura di), *GDPR e Normativa Privacy Commentario,* Milano, Ipsoa, pp.881-904

di Somma C. (2019), Trattamento in ambito pubblico e comunicazioni al Garante, *Privacy&Data Protection Technology Cybersecurity*, n. 2/2019, pp.13-16

El Emam K., Mosquera L., Hoptroff R. (2020) *Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data*, Sebastopol, O'Reilly Media

Foà S. (2026), L'altruismo dei dati e le sue potenzialità per l'interesse generale: dal Data governance act al diritto interno*,* in Cavallaro M.C. Fant V. (a cura di), *Ia Sanità - Territorio - Pubbliche Amministrazioni,* Napoli, Editoriale scientifica, pp.523-539

Franca S. (2023), *I dati personali Nell'amministrazione pubblica. Attività di trattamento E tutela del privato,* Napoli, Editoriale scientifica

Francario F. (2022), Protezione dei dati e pubblica amministrazione, in Pisani C., Proia G., Topo A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro,* Milano, Giuffrè, pp.679-722

Garofoli R., Ferrari G. (2008), *Manuale di diritto amministrativo*, Roma, Nel Diritto editore, pp.3 e ss.

He Z. (2023), From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law, *Digital Society*, n.2, art.17

Lee P. (2025), Synthetic Data and the Future of AI, *Cornell Law Review*, 110, n.1, pp.1-74

Longo E. (2017), I trattamenti nel settore dell'istruzione e a fini di ricerca (scientifica, storica, statistica), in Califano L., Colapietro C. (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, Editoriale scientifica, pp.491-508

Yermilov O., Raheja V., Chernodub A. (2023), Privacy- and Utility-Preserving NLP with Anonymized data: A case study of Pseudonymization, in *Proceedings of the 3rd Workshop on Trustworthy Natural Language Processing (TrustNLP 2023)*, Toronto, Association for Computational Linguistics, pp.232-241

Patti L. (2019), Art. 58/Regolamento UE 2016/679, in D'Agostino A., Barlassina L.R., Colarocco V. (a cura di), *Commentario al Regolamento UE 2016/679 e al Codice della Privacy aggiornato*, Vignate, Top Logal Academy, pp.460-468

Ponti B. (2023), *Attività amministrativa e trattamento dei dati personali,* Milano, Franco Angeli

Simonati A. (2023), Il trattamento di dati personali e gli accessi amministrativi "generali": le dinamiche frontiere della discrezionalità, *Diritto Amministrativo*, 31, n.1, pp.3-27

Stalla-Bourdillon S. (2025), The state of pseudonymisation in the EU: Where do we stand today?, *Privacy and Data Protection,* 18, n.2, pp.4-8

Stefanelli S. (2018), Trattamento di dati personali per scopi di ricerca scientifica, in Cassano G., Colarocco V., Gallus G.B., Micozzi F.P. (a cura di), *Il processo di adeguamento al GDPR*, Milano, Giuffré Francis Lefebvre, pp.369-399

Trubiani F. (a cura di) (2025), *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, Giappichelli, Torino

Chiara di Somma
C.DiSomma@gpdp.it
Giurista esperta in protezione dei dati personali, funzionario presso l'Autorità Garante per la protezione dei dati personali dal 2009. Nel corso della sua formazione ha conseguito un Master di II Livello in Tutela dei Diritti umani presso l'Università Sapienza di Roma (2004) ed un Dottorato di ricerca in Diritto pubblico e costituzionale presso l'Università Federico II di Napoli (2008). Oltre alle numerose docenze nell'ambito di Master universitari e corsi di formazione in tema di protezione dei dati personali è cultrice della materia presso l'Università Luiss Guido Carli (corso di Diritto digitale e tutela dei dati), Corso di Laurea Magistrale in Giurisprudenza A.A. 2025-2026. È inoltre autrice di numerose pubblicazioni scientifiche in ambito giuridico nel settore della protezione dei dati personali.