

## The impact of GDPR on the access to archives and the creation of finding aids

Stefano Allegrezza<sup>(a)</sup>

a) Università degli Studi di Bologna

Contact: Stefano Allegrezza, [stefano.allegrezza@unibo.it](mailto:stefano.allegrezza@unibo.it)

Received: 15 April 2023; Accepted: 21 June 2023; First Published: 15 September 2023

### ABSTRACT

The General Data Protection Regulation (GDPR) and the Personal Data Protection Code, which has been updated to comply with the principles of the Regulation, have produced significant consequences with regard to the access to archives and the creation of finding aids, which must be subject to certain rules in order to comply with the principles laid down and avoid sanctions. Without claiming to be exhaustive, given the complexity and vastness of the topic, the proposed contribution aims to provide an overview of the situation on this issue, which is still in many ways little known, by offering some thoughts on the key principles of the GDPR and their application to the archival context of access and description.

### KEYWORDS

GDPR; Archives; Access; Finding aids; Personal Identifiable Information.

## L'impatto del GDPR sulla consultabilità degli archivi e la produzione di strumenti di descrizione archivistica

### ABSTRACT

Il Regolamento generale sulla protezione dei dati (GDPR) e l'adeguamento del Codice in materia di protezione dei dati personali ai principi del Regolamento, hanno prodotto delle conseguenze rilevanti per quanto riguarda la consultabilità degli archivi e la produzione degli strumenti di descrizione archivistica, che devono sottostare a determinate regole al fine di rispettare i principi previsti ed evitare sanzioni. Pur senza alcuna pretesa di esaustività, stante la complessità e la vastità dell'argomento, il contributo intende affrontare questo tema, ancora per molti versi poco conosciuto, fornendo alcuni spunti di riflessione sui principi chiave del GDPR e sulla loro applicazione al contesto della consultabilità e della descrizione archivistica.

### PAROLE CHIAVE

GDPR; Archivi; Consultabilità; Strumenti di ricerca; Mezzi di corredo; Dati personali.

## Introduzione e quadro normativo

Quando, il 25 maggio 2018, il Regolamento UE 2016/679, *Regolamento generale sulla protezione dei dati* – comunemente noto come GDPR, General Data Protection Regulation – divenne applicabile, nelle Istituzioni archivistiche si scatenò una vera e propria ondata di ‘panico’. In molti si chiesero se le nuove norme europee sulla protezione dei dati personali, nate per proteggere i cittadini dalla crescente invadenza dei giganti del web sarebbero state compatibili con il compito loro affidato della conservazione, consultazione e valorizzazione o se non avrebbero piuttosto prodotto come conseguenza lo ‘svuotamento’ degli archivi del futuro (Barrera 2018c). Le fondazioni, gli istituti culturali, le imprese e gli altri soggetti privati avrebbero potuto continuare ad acquisire e conservare archivi storici contenenti dati personali o gli sarebbe stato proibito dal GDPR? Queste ed altre erano le domande che circolavano all’epoca e che tutt’oggi molti continuano a porsi. Per rispondere a tali interrogativi è necessario avere ben chiaro il quadro normativo. Innanzitutto vanno ricordati gli articoli 9 e 21 della Costituzione Italiana che garantiscono il fondamentale diritto alla ricerca e all’informazione<sup>1</sup>; va poi ricordata la disciplina sulla consultabilità dei documenti “per scopi storici” che oggi è regolata in via generale dal *Codice dei beni culturali e del paesaggio* (emanato con il d.lgs. del 22 gennaio 2004 n. 42 e conosciuto anche come codice Urbani dal nome dell’allora Ministro dei beni e delle attività culturali Giuliano Urbani), il quale dedica uno specifico Capo a questo tema all’interno del Titolo II dedicato alla fruizione e valorizzazione dei beni culturali, ossia al loro godimento pubblico; va poi tenuto in considerazione il *Codice in materia di protezione dei dati personali* (noto come “Codice della privacy”) emanato con il d.lgs. 30 giugno 2003, n. 196, in vigore dal 1° gennaio 2004, insieme con le *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica* che ne costituiscono l’Allegato A.3 (GPDP 2018)<sup>2</sup>. Di fondamentale rilevanza il già citato Regolamento UE 2016/679, al quale il *Codice in materia di protezione dei dati personali* si è adeguato con la pubblicazione del d. lgs. 10 agosto 2018, n. 101. Non c’è dubbio che il Regolamento europeo<sup>3</sup> sia una norma di non facile lettura: consta di 99 articoli, preceduti da ben 173 “considerando”, che hanno solo un valore interpretativo della norma, scritti in un linguaggio che può risultare ostico, specialmente nella traduzione

---

<sup>1</sup> In particolare l’art. 9 («La Repubblica promuove lo sviluppo della cultura e la ricerca scientifica e tecnica») e l’art. 21 («Tutti hanno diritto di manifestare liberamente il proprio pensiero con la parola, lo scritto e ogni altro mezzo di diffusione»).

<sup>2</sup> Le nuove *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica* sostituiscono il precedente *Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici* (che, in precedenza, costituiva l’allegato A.2 al *Codice in materia di protezione dei dati personali*). Le Regole deontologiche non sono un semplice regolamento ma sono state elevate dall’art. 2-quater c. 4 del *Codice in materia di protezione dei dati personali* a fonte normativa subordinata solo alla legge: «Il rispetto delle disposizioni contenute nelle regole deontologiche [...] costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali». Per gli archivisti, le Regole deontologiche costituiscono la bussola che deve sempre orientarne il comportamento, quando trattano dati personali.

<sup>3</sup> Nell’ordinamento della UE, i regolamenti sono l’equivalente di ciò che per gli Stati membri sono le leggi: sono direttamente applicabili in tutti i Paesi membri, in tutte le loro parti, e non necessitano di recepimento: gli Stati membri non devono adottare provvedimenti per la loro attuazione (a differenza di ciò che avviene per le direttive) ed è attuato allo stesso modo in tutti gli Stati dell’Unione senza margini di libertà nell’adattamento. Però il GDPR ha lasciato ai Paesi membri l’autonomia di regolare alcune materie, fra cui le deroghe in caso di “archiviazione nel pubblico interesse”. È, dunque, necessario che gli archivisti, oltre al GDPR, conoscano la normativa nazionale.

italiana<sup>4</sup>. Forse è anche per questo che lo *European Archives Group*<sup>5</sup> ha ritenuto opportuno redigere la *Guida alla protezione dei dati personali per gli archivi*, pubblicata, nella versione in lingua inglese, il 26 ottobre 2018 (European Archives Group 2018)<sup>6</sup>. Dal 12 marzo 2019, il documento è disponibile anche in lingua italiana, grazie alla traduzione curata dalla Direzione generale archivi (traduzione e note all'edizione italiana di Giulia Barrera e Caterina Fontanella). Pur non avendo forza normativa, queste linee guida vanno tenute in considerazione perché forniscono le informazioni minime indispensabili che tutti gli archivisti dovrebbero conoscere e costituiscono una sorta di 'vademecum' sul Regolamento europeo esplicitamente indirizzato agli archivisti. Infine, va ricordata la *Carta dei diritti fondamentali dell'Unione europea* che sancisce, con l'art. 8, il diritto per ciascun individuo alla protezione dei dati di carattere personale che lo riguardano. Come si può intuire, si tratta di un complesso di norme molto articolato, caratterizzato da una continua evoluzione sia in ambito nazionale che europeo soprattutto a livello di giurisprudenza, spesso di difficile od incerta interpretazione e che non rendono affatto semplice individuare principi e regole generali che possano essere applicate sic et simpliciter al contesto archivistico.

## Iniziative e convegni sul tema

Per questo motivo, soprattutto all'inizio, il tema dell'impatto del GDPR sull'accesso e la consultabilità degli archivi è stato affrontato in alcuni importanti incontri, tra cui meritano senz'altro una segnalazione la giornata di studi *La conservazione archivistica nell'era del GDPR: il nodo degli archivi privati e dei dati penali* che si è tenuta il 30 gennaio 2019 a Roma nella sala Spadolini del Ministero per i Beni e le attività culturali, su iniziativa della DGA, dell'ANAI e dell'ICAR e che si è occupata specificatamente del trattamento dei dati personali relativi a condanne penali e reati; l'incontro di studio *Il GDPR in archivio: strumenti di lavoro per l'applicazione del Regolamento europeo sulla protezione dati personali* organizzato dalla DGA, dall'ANAI e dall'Archivio Centrale dello Stato e tenutosi il 13 marzo 2019 presso lo stesso Istituto in occasione della III edizione della Settimana dell'Amministrazione aperta; il Seminario di aggiornamento dal titolo *Consultabilità e protezione dei dati personali. Normativa italiana ed europea, giurisprudenza e deontologia professionale* organizzato dall'Archivio di Stato di Torino, dalla Scuola di archivistica, paleografia e diplomatica dello stesso, dall'Associazione Amici dell'Archivio di Stato di Torino, dalla Soprintendenza archivistica e bibliografica del Piemonte e della Valle d'Aosta, dall'ANAI – Sezione Piemonte e Valle d'Aosta e tenutosi online il 10 febbraio 2021. Anche all'estero il tema della relazione tra GDPR e archivi è stato oggetto di numerose iniziative: basti ricordare, una tra tutte, il convegno *Personal data in the archives: privacy and openness in the information age* ospitato dall'Archivio di Stato Regionale di

<sup>4</sup> Su alcuni errori di traduzione nel passaggio del GDPR dalla versione inglese alla versione italiana si veda Barrera (2018a).

<sup>5</sup> Lo *European Archives Group* (EAG) è il gruppo di coordinamento delle Direzioni Generali Archivi e/o degli Archivi Nazionali dei Paesi dell'Unione Europea, creato dalla Commissione europea nel 2006. Lo EAG ha seguito molto attentamente, sin dal 2012, il complesso iter di approvazione del Regolamento, facendo intensa attività di lobbying a favore degli Archivi ed ottenendo risultati importanti. Nell'iniziale schema di Regolamento, non veniva prevista alcuna eccezione a favore degli archivi; nel testo approvato, buona parte di obblighi e divieti prevedono eccezioni a favore degli Archivi (Barrera 2018c).

<sup>6</sup> Le Linee guida si occupano del trattamento dei dati personali presenti nei documenti conservati negli archivi storici, sia pubblici che privati.

Praga e dall'Archivio Nazionale della Repubblica Ceca il 9 novembre 2021 e al quale ha partecipato Giulia Barrera in rappresentanza dell'Italia. Occorre, tuttavia, riconoscere che dopo l'interesse iniziale, manifestatosi a ridosso della pubblicazione del GDPR e dei regolamenti collegati, il tema non è stato più oggetto di iniziative e convegni, come se fosse ormai dato acquisito, e questo ha contribuito all'insorgere nel tempo di uno stato di incertezza sulla sua applicazione.

## I principi generali ai quali attenersi nella descrizione degli archivi

Tornando all'oggetto principale di questo contributo, ovvero l'impatto del GDPR sulla consultabilità degli archivi e sulla descrizione archivistica, il primo elemento che occorre tener presente è che tali attività determinano normalmente il *trattamento*<sup>7</sup> di dati personali<sup>8</sup>. Infatti, le fonti utilizzate dagli storici per le ricerche scientifiche sono per loro stessa natura ricche di dati personali e «non potrebbe essere altrimenti perché la storia si occupa delle vicende relative alle persone» (Bonfiglio-Dosio 2023, 178). Quindi, rientrano pienamente nel campo di applicazione del GDPR del quale devono rispettare i principi generali stabiliti dall'art. 5: il principio di «liceità, correttezza e trasparenza» (i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato); il principio di «limitazione della finalità» (i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità); il principio di «minimizzazione dei dati» (il trattamento dei dati personali deve essere adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali i dati personali sono trattati); il principio di «esattezza» (i dati personali devono essere

---

<sup>7</sup> L'art. 4 del GDPR definisce «trattamento» qualsiasi «operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

<sup>8</sup> Il Codice della privacy, antecedentemente alle modifiche apportate dal d.lgs. 101/2018 di adeguamento al GDPR, distingueva, con l'art. 4, tra *dati personali* («qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale»), *dati personali sensibili* (cioè «i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale»), e *dati personali giudiziari* (cioè «i dati personali idonei a rivelare provvedimenti di cui all'art. 3, c. 1, lettere da a) a o) e da r) a u), del d.p.r. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale»). Nella prassi i dati personali «idonei a rivelare lo stato di salute, la vita sessuale», venivano detti *sensibilissimi* e il Codice dei Beni culturali vi aveva aggiunto la categoria dei dati personali relativi ai «rapporti riservati di tipo familiare», che diventano consultabili 70 anni dopo la loro data. Queste espressioni non compaiono più nel GDPR, sostituite dalla definizione di *dato personale*, inteso come «qualsiasi informazione riguardante una persona fisica identificata o identificabile» (art. 4) e *dato personale particolare*, ovvero quel dato personale che riveli «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale», nonché i «dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (art. 9). In sostanza, si tratta di quelli che in passato venivano chiamati «dati sensibili» e «dati sensibilissimi», con l'aggiunta della categoria dei dati genetici e biometrici. Il GDPR non usa più neppure l'espressione «dati personali giudiziari», sostituita da «dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza» (art.10).

esatti e, se necessario, aggiornati; inoltre, devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati); il principio di “limitazione della conservazione” (i dati personali devono essere 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); il principio di “integrità e riservatezza” (i dati personali devono essere trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali); il principio di “responsabilizzazione” (il titolare del trattamento è competente per il rispetto dei principi generali appena visti e in grado di provarlo). Nel seguito, pur senza pretesa alcuna di esaustività, cercheremo di delineare le principali conseguenze che l’applicazione di questi principi produce sulla consultabilità e sulla descrizione degli archivi.

## **Il principio della liceità del trattamento**

Il primo principio che occorre rispettare nel trattamento dei dati personali è quello della liceità: il trattamento è lecito solamente se si verifica almeno una delle condizioni previste dall’art. 6: “l’interessato ha espresso il consenso al trattamento dei propri dati personali”; “il trattamento è necessario per l’esecuzione di un contratto di cui l’interessato è parte”, “il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento”, e così via. Di particolare interesse per gli archivisti è la condizione posta al c. 1, lett. e), che stabilisce che il trattamento dei dati personali è lecito se “è necessario per l’esecuzione di un compito di interesse pubblico”. La definizione di quali tipi di compiti siano da considerarsi “di pubblico interesse” viene lasciata dal GDPR alla normativa dell’Unione europea o alle leggi nazionali<sup>9</sup>. La legge degli Stati membri può, ad esempio, definire la conservazione degli archivi da parte di una specifica Istituzione o la conservazione di determinate categorie di archivi come “compito di interesse pubblico” rendendone così lecito il trattamento.

## **Il principio di limitazione della conservazione e il trattamento per fini di pubblico interesse**

Uno dei principi cardine del GDPR è quello della limitazione della conservazione: i dati personali raccolti e trattati dovrebbero essere “conservati in una forma che consenta l’identificazione degli interessati” (ovverosia le persone a cui si riferiscono i dati) solamente per il tempo necessario a raggiungere lo scopo per il quale sono stati raccolti (art. 5.1., e). Se questo principio non ammettesse eccezioni, negli archivi non potrebbero più esserci documenti che contengono dati personali.

---

<sup>9</sup> Va tenuto presente che le deroghe a favore della “archiviazione nel pubblico interesse” riguardano solo i trattamenti dei dati personali contenuti nei fondi archivistici conservati dagli Archivi. Tutti gli altri trattamenti di dati personali effettuati dagli Archivi ricadono sotto le stesse regole che si applicano a qualsiasi altro ente pubblico o privato. In altre parole, quando un Istituto archivistico tratta i dati personali relativi agli impiegati, ai collaboratori esterni, agli utenti, agli studenti che partecipano ad attività didattiche e così via, non è possibile godere di alcuna deroga.

I legislatori europei hanno però introdotto delle deroghe a questa regola. Infatti, lo stesso GDPR stabilisce che “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”, purché si assumano specifiche misure «a tutela dei diritti e delle libertà dell’interessato» (art. 5.1 e). Quindi vi sono almeno due deroghe che sono rilevanti per gli archivi, una nel caso di trattamento per finalità di archiviazione nel pubblico interesse e l’altra nel caso di trattamento per finalità di ricerca scientifica o storica. Non è certamente questa la sede opportuna per addentrarci in una approfondita disamina della definizione di “archiviazione nel pubblico interesse”, tuttavia è importante fornire almeno alcuni elementi di base. Innanzitutto occorre domandarsi quali siano gli enti che trattano dati personali per “finalità di archiviazione nel pubblico interesse”. Il considerando 158 spiega il significato di questa espressione: si tratta di quegli enti, pubblici o privati, che, in virtù del diritto dell’Unione europea o di quello degli Stati membri, hanno l’obbligo legale di «acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a documenti con un valore a lungo termine per l’interesse pubblico generale». Ci si può chiedere, allora, quali siano gli enti che rientrano nella definizione appena letta. La risposta non è immediata. Occorre osservare, infatti, che ciò che rileva non è la natura degli archivi, ma il mandato dell’Istituzione che li conserva, che discende da un obbligo legale. Con riferimento alla situazione italiana, di certo rientrano in questa categoria gli Archivi di Stato, gli Archivi dei comuni, gli Archivi delle Regioni, ed in generale gli Archivi degli Enti pubblici sia statali che non statali (si pensi all’INPS o alle Camere di Commercio); vi rientrano anche, in generale, tutte quelle istituzioni, anche private, che conservano archivi e alle quali la legge ha affidato il compito di acquisire, conservare e rendere accessibili ai ricercatori documenti contenenti dati personali: si pensi alle numerose Istituzioni che conservano le carte personali di scrittori, personaggi politici, scienziati, eminenti personalità in generale. Riguardo la seconda deroga, va tenuto presente che, sebbene non tutti i soggetti conservatori abbiano l’obbligo legale di acquisire archivi (e dunque non rientrano nella prima deroga), tuttavia, in molti casi, tali soggetti hanno una chiara missione culturale e conservano archivi a fini di ricerca storica, e quindi rientrano a pieno titolo nella seconda deroga.

## Il principio di minimizzazione dei dati

Un altro principio chiave del GDPR è quello della minimizzazione dei dati: i dati personali devono essere raccolti e trattati solamente se è davvero necessario farlo. Anche la produzione di strumenti di ricerca deve rispettare questo principio; ad esempio, quando si descrivono fondi archivistici che contengono dati su persone viventi relativi allo stato di salute, alla vita sessuale, alle opinioni politiche o ad altre categorie particolari di dati, oppure riguardanti le condanne penali, una buona soluzione per essere conformi al principio di minimizzazione è quella di creare due inventari, uno con i nomi reali – al fine di poter rispondere a una eventuale richiesta d’accesso da parte degli interessati e permettere loro di esercitare gli altri diritti riconosciuti dal GDPR –, ed uno in cui i nomi sono sostituiti da *pseudonimi*<sup>10</sup>, da utilizzare per finalità di ricerca e pubblicabile

---

<sup>10</sup> La *pseudonimizzazione* è una misura di sicurezza introdotta ufficialmente dal GDPR, che la definisce come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l’utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e

online. Questo significa, anche, utilizzare software per la descrizione archivistica che consentano di creare di due differenti versioni di un inventario – una con pseudonimi ed una con i nomi reali – se si vuole essere conformi al GDPR. Caso per caso, poi, gli archivisti dovranno valutare come meglio bilanciare l’obbligo di descrivere, comunicare, promuovere, diffondere e fornire accesso ad archivi selezionati per la conservazione permanente (considerando 158) con il principio della minimizzazione dei dati (art. 5), che richiede di limitare il trattamento dei dati allo strettamente necessario. Anche le operazioni di selezione e scarto, ovvero «la distruzione consapevole e motivata di una grande quantità di documentazione non rilevante ai fini della ricerca che è condizione per la salvaguardia dei documenti che vengono conservati perché di interesse storico» (Carucci 2021, 262) rientra nel concetto di minimizzazione dei dati.

### **Il trattamento di categorie “particolari” di dati personali (art. 9)**

La produzione di strumenti di descrizione archivistica implica spesso il trattamento di documenti contenenti *dati personali particolari* (cfr. nota 9). L’art. 9, c. 1 del GDPR accorda una particolare protezione a questa categoria di dati personali, il cui trattamento potrebbe generare un alto rischio per i diritti e le libertà fondamentali degli interessati, vietandone in linea generale il trattamento. Tuttavia, anche in questo caso, se il GDPR non ammettesse delle deroghe, il lavoro degli archivisti ne risulterebbe gravemente menomato ed in molti casi non sarebbe possibile produrre strumenti di ricerca. Fortunatamente, il GDPR ammette delle deroghe anche a questa norma. Il divieto di trattare queste categorie particolari di dati personali non si applica se “il trattamento è necessario a fini di archiviazione nel pubblico interesse” o a fini “di ricerca scientifica o storica”. Tale trattamento deve trovare fondamento in una norma giuridica ed essere “proporzionato alla finalità perseguita”; inoltre deve rispettare “l’essenza del diritto alla protezione dei dati” e prevedere “misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell’interessato” (art. 9, c. 2, lett. j). Nei Paesi membri dell’Unione Europea, le leggi nazionali escludono dalla consultazione i documenti contenenti categorie particolari di dati personali, per periodi che variano da pochi decenni a oltre un secolo. In Italia, l’art. 122 Codice dei beni culturali e del paesaggio (d.lgs. 22 gennaio 2004, n. 42) fissa i termini di consultabilità dei documenti conservati negli Archivi di Stato e negli archivi storici degli enti pubblici: «I documenti conservati negli archivi di Stato e negli archivi storici delle regioni, degli altri enti pubblici territoriali nonché di ogni altro ente ed istituto pubblico sono liberamente consultabili, ad eccezione: a) di quelli dichiarati di carattere riservato, ai sensi dell’art. 125, relativi alla politica estera o interna dello Stato, che diventano consultabili cinquanta anni dopo la loro data; b) di quelli contenenti i dati sensibili nonché i dati relativi a provvedimenti di natura penale espressamente indicati dalla normativa in materia di trattamento dei dati personali, che diventano consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare». Gli archivisti, dunque, hanno già una lunga e consolidata esperienza nell’applicazione di leggi che limitano l’accesso alle categorie particolari di dati personali.

---

soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile».

## **Il trattamento dei dati personali relativi a condanne penali e reati (art. 10)**

Un'altra categoria di dati personali che è possibile incontrare, soprattutto in determinati ambiti, è quella relativa a condanne penali e reati<sup>11</sup>. Il GDPR pone rigide limitazioni al trattamento di questa categoria di dati personali che “deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati” (art. 10). Nei Paesi membri dell'Unione Europea, le leggi nazionali stabiliscono che dopo un certo numero di anni – generalmente compresi tra 20 o 30 – la documentazione processuale e giudiziaria selezionata per la conservazione permanente sia versata agli Archivi di Stato o ad altre istituzioni archivistiche. Di solito la documentazione viene sottoposta ad interventi di riordinamento ed inventariazione per renderla accessibile ai ricercatori, e quindi si configurano dei trattamenti di grandi quantità di dati personali relativi a condanne penali e reati. Questi trattamenti sono pienamente conformi al GDPR, in quanto sono previsti dalla legge ed effettuati da autorità pubbliche con appropriate garanzie per i diritti e le libertà degli interessati. Se ad esempio la legislazione nazionale limita l'accesso alla documentazione giudiziaria per un certo numero di anni, gli archivisti applicano scrupolosamente questo tipo di restrizione (European Archives Group 2018). Se si pubblicano online, liberamente accessibili, strumenti di descrizione archivistica relativi a documenti contenenti dati personali “relativi a condanne penali e reati” ed esiste la possibilità che le persone interessate siano ancora in vita, è opportuno adottare precauzioni come la pubblicazione in un'area del sito accessibile solo previa registrazione (quindi non indicizzabile da parte dei motori di ricerca) o ricorrere a tecniche come quella dell'*anonimizzazione* o dell'*oscuramento* applicate ai dati personali in modo tale che le persone fisiche interessate non possano più essere identificate in nessun modo. Caso per caso, gli archivisti dovranno valutare come meglio bilanciare il loro obbligo legale di “descrivere, comunicare, promuovere, diffondere e fornire accesso” agli archivi selezionati per la conservazione permanente (considerando 158) con il principio della minimizzazione dei dati (art. 5), che richiede di limitare il trattamento dei dati allo strettamente necessario e in ossequio al principio fondamentale del rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate. Ad ogni modo è sempre opportuno contattare la propria autorità garante (in Italia, il Garante per la protezione dei dati personali) e chiedere istruzioni su quali siano le misure più consone da adottare per la salvaguardia dei diritti e delle libertà degli interessati.

## **Il diritto alla cancellazione («diritto all'oblio») (art. 17)**

Uno dei diritti che più di tutti ha suscitato la preoccupazione degli archivisti è il cosiddetto “diritto all'oblio”, la cui esistenza nell'ambito della Unione Europea è stata affermata per la prima volta nel 2014 da un'epocale sentenza della Corte di giustizia della Unione Europea sul famoso caso Google Spagna<sup>12</sup>. Il GDPR usa la stessa espressione nel titolo dell'art. 17 “Diritto alla cancellazione («Di-

<sup>11</sup> Per un approfondimento su questo particolare punto si veda Barrera (2018b).

<sup>12</sup> Si tratta della sentenza con la quale la Corte europea aveva ordinato a Google Spagna di rimuovere dai risultati delle ricerche le notizie riguardanti un caso di bancarotta accaduto a un cittadino spagnolo, Mario Costeja Gonzales. Le notizie erano state legittimamente pubblicate da un quotidiano nel 1998 ma a distanza di diversi anni apparivano ancora tra i primi risultati quando si cercava il nome di Costeja. La sentenza della Corte di giustizia non ha coinvolto gli archivi analogici e

ritto all'oblio»<sup>13</sup>). Tuttavia, a differenza della sentenza poc'anzi citata, nel GDPR, il diritto all'oblio non si riferisce alla deindicizzazione, ma alla vera e propria cancellazione dei dati personali. L'art. 17 consente, infatti, all'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano. Tale diritto può essere esercitato quando “i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti” o quando “l'interessato revoca il consenso” al loro trattamento, oltre ad altre circostanze. Anche in questo caso, tale diritto è soggetto a diverse limitazioni, grazie alle quali il trattamento di dati personali contenuti nei documenti per finalità connesse con la produzione di strumenti di ricerca è lecito. Ad esempio, il diritto all'oblio non si applica se il trattamento è necessario per “l'adempimento di un obbligo legale”, per “l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento” oppure “a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici” se la cancellazione rischia “di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento” (art. 17, c. 3).

Il considerando 158 del GDPR fornisce ulteriori indicazioni: le pubbliche autorità e gli altri enti che conservano archivi nel pubblico interesse hanno “l'obbligo legale” di trattare archivi selezionati per la conservazione permanente e la cancellazione di dati personali contenuti in documenti archivistici renderebbe impossibile, per questi enti, assolvere alla missione istituzionale assegnatagli dalla legge. Il diritto alla cancellazione non si applica, dunque, ai documenti selezionati per la conservazione permanente da Archivi che rientrano nella definizione del considerando 158 (Barrera 2019). Allo stesso tempo, gli archivisti dovrebbero ricordare che il diritto all'oblio, così come affermato dalla Corte di giustizia della Unione Europea (cioè non cancellazione, ma deindicizzazione dei dati personali), può essere messo in pratica dagli Archivi senza pregiudicare i loro compiti istituzionali (European Archives Group 2018). Deindicizzare o rimuovere un link, o prevenire in ogni altro modo la ricerca di nomi all'interno dei documenti da parte dei motori di ricerca, non compromette, infatti, l'integrità dei documenti d'archivio e non mette a rischio la loro conservazione permanente.

Per quanto riguarda gli strumenti di ricerca contenenti dati personali relativi a persone in vita, se la loro diffusione può mettere a rischio la dignità degli interessati gli archivisti dovrebbero astenersi dal pubblicarli online. Inoltre, dovrebbero valutare – in relazione alla natura dei dati personali – l'opportunità di pubblicarli in un'area del loro sito web ad accesso riservato, non indicizzabile da parte dei motori di ricerca (European Archives Group 2018). In quest'ultimo caso si tratterebbe, infatti, di “comunicazione” dei dati personali e non più di “diffusione”, una distinzione fondamentale che occorre tenere bene a mente<sup>13</sup>. Per quanto riguarda la diffusione (che può riguardare, ad esempio, la pubblicazione online di strumenti di ricerca) non basta rispettare le limitazioni temporali relative alla consultabilità dei documenti contenenti dati personali ex “sensibili” (convinzioni politiche, filosofiche, religiose, adesione a partiti e sindacati, etc. ) – che risul-

---

digitali del quotidiano, che sono rimasti ‘intatti’, ma ne ha imposto la *deindicizzazione*, ovvero ha richiesto che tra i risultati che appaiono cercando su Google il nome di Costeja non comparissero quelli sulla bancarotta (le notizie sono tuttora rintracciabili utilizzando altre chiavi di ricerca).

<sup>13</sup> Secondo il Codice della Privacy, art. 2-ter, c. 4, si intende per “comunicazione”, il «dare conoscenza dei dati personali a uno o più soggetti *determinati* diversi dall'interessato [...] in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione» e per “diffusione”, il «dare conoscenza dei dati personali a soggetti *indeterminati*, in qualunque forma, anche mediante la loro messa a disposizione o consultazione».

tano non consultabili per quaranta anni – e quelle relative ai documenti contenenti dati personali ex ‘sensibilissimi’ (stato di salute, abitudini sessuali e informazioni che riguardano l’intimità della vita familiare) – che non sono consultabili per settanta anni – ma bisogna andare molto cauti e fare qualche riflessione in più. Infatti, occorre tenere in considerazione che, ancorché siano trascorsi tali termini, tali documenti potrebbero non essere pubblicabili – potendo la loro diffusione ledere il principio del rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, dei loro eredi o di terze persone coinvolte, che si estende ben oltre i limiti temporali quarantennali e settantennali che la normativa prevede (Twardzik 2014) – se non dopo essere stati eventualmente sottoposti ad interventi di anonimizzazione o pseudonimizzazione. Caso per caso, gli archivisti dovranno valutare come meglio bilanciare il loro obbligo legale di “descrivere, comunicare, promuovere, diffondere e fornire accesso” ad archivi selezionati per la conservazione permanente (considerando 158) con il principio della minimizzazione dei dati (art. 5), che richiede di limitare il trattamento dei dati allo strettamente necessario.

### **Il trattamento di dati personali relativi a persone defunte**

Quando si descrivono gli archivi si possono incontrare dati personali sia di persone in vita che di persone decedute. Il GDPR protegge i dati personali delle persone viventi ma non detta regole inerenti i dati personali delle persone defunte. Ma come possono gli archivisti sapere se una persona è deceduta (nel qual caso il GDPR non si applica), oppure è ancora in vita e quindi si devono porre in essere tutte le accortezze e le cautele previste dal GDPR per il trattamento dei dati personali? In molti casi ciò non è possibile, ma si può ragionevolmente presumere che persone nate più di cento anni fa siano morte. Se, per esempio, un archivistista sta descrivendo un fondo archivistico dove vi sono documenti personali di soldati che hanno combattuto la Prima guerra mondiale, può dare per scontato che nessuno di essi sia ancora in vita e che dunque il GDPR non si applichi a questi documenti. In molti casi, tuttavia, la situazione non è così chiara e sarà necessario valutare caso per caso la possibilità che i fondi archivistici oggetto di descrizione possano contenere dati relativi a persone viventi.

Ad ogni modo, il GDPR lascia alla legislazione dei singoli Stati membri la possibilità di legiferare in materia di protezione dei dati personali di persone defunte. Questo è proprio il caso dell’Italia che con l’art. 2-terdecies («Diritti riguardanti le persone decedute») del Codice della Privacy<sup>14</sup>, nonché con le Regole deontologiche (art. 7 c. 3 e *passim*)<sup>15</sup>, ha riconosciuto la possibilità di esercitare i diritti delle persone decedute di cui agli articoli da 15 a 22 del GDPR (fra cui, il diritto di

---

<sup>14</sup> L’ art. 2-terdecies è stato inserito nel Codice della Privacy con il d.lgs. 101/2018. La norma in questione stabilisce pure che l’esercizio di questi diritti non è ammesso, limitatamente ai servizi della società dell’informazione (ad esempio, un account su una piattaforma digitale), quando l’interessato lo ha espressamente vietato con dichiarazione scritta comunicata al titolare del trattamento.

<sup>15</sup> Infatti, il considerando 27 del GDPR stabilisce che «Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute». Com’è noto, l’art. 122 del d.lgs. 42/2004, relativo alla consultabilità dei documenti d’archivio, prevede l’esclusione dalla consultazione per 40 o 70 anni dei documenti contenenti determinate categorie di dati personali, indipendentemente dall’esistenza in vita o meno dell’interessato; implicitamente, dunque, anche il Codice dei beni culturali prevede la tutela dei dati personali dei defunti, se di data più recente rispetto ai termini di consultabilità.

accesso ai dati personali, di rettifica o cancellazione, di limitazione del trattamento) a chi “ha un interesse proprio, o agisce a tutela dell’interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione”, come avviene spesso nel caso degli eredi. Quindi nella produzione di strumenti di ricerca occorrerà tener presente la possibilità che anche qualora nei documenti i dati personali fossero relativi a persone non più in vita, i relativi diritti possano essere esercitati dagli eredi o da altri soggetti legittimati.

## Conclusioni

La questione della consultabilità degli archivi e della produzione di strumenti di ricerca alla luce degli obblighi introdotti dal GDPR è sicuramente una delle più complesse da affrontare per la disciplina archivistica, dal momento che occorre contemperare diritti contrapposti, quali il diritto all’informazione e alla ricerca da una parte e il diritto alla riservatezza e alla privacy dall’altra. La complessità deriva anche dalla grande quantità di norme che devono essere prese in considerazione e che delineano un quadro normativo a volte disorganico, con disposizioni di legge non sempre tra loro coordinate ed a volte persino contraddittorie. In aggiunta, in ambiente digitale, i problemi dell’accesso sono aggravati dalla quantità, varietà e complessità dei documenti elettronici: in molti casi, grandi masse di documenti non potranno essere controllate e verificate manualmente prima dell’accesso, per cui le garanzie e i controlli dovranno essere sempre più automatizzati, magari ricorrendo ad applicazioni basate su tecniche di intelligenza artificiale. Anche la pianificazione di nuovi sistemi di gestione documentale da parte di enti pubblici i cui archivi saranno in futuro versati agli Archivi di Stato o alle Separate sezioni di archivio deve tener conto della necessità di essere conformi al GDPR fin dalla fase della progettazione (privacy by design). A questo proposito è importante assumere un atteggiamento proattivo e coinvolgere le istituzioni archivistiche nelle fasi iniziali della definizione dei sistemi, per garantire che, al momento opportuno, i documenti possano essere estratti dal sistema per essere poi versati in Archivio conformemente alle previsioni del GDPR. Ad ogni modo, non si può prescindere dalla necessità di operare uno scrupoloso controllo su quanto si prevede di pubblicare o di descrivere – anche ricorrendo alle opportune tecniche di anonimizzazione e pseudonimizzazione nella produzione di strumenti di ricerca – per cercare di trovare un equilibrio tra il compito di promuovere l’accesso alle fonti e l’obbligo di rispettare la dignità delle persone e i diritti fondamentali delle persone.

## Riferimenti bibliografici

- Barrera, Giulia. 2018a. "Lost in translation: Errori di traduzione nel Regolamento europeo protezione dati personali." *Il Mondo degli archivi*. 29 ottobre 2018. <https://tinyurl.com/zaaj2z2b>.
- Barrera, Giulia. 2018b. "Il trattamento a fini di ricerca dei dati personali relativi a condanne penali e reati. A proposito del GDPR." *Rivista di studi e ricerche sulla criminalità organizzata*. 4(4): 5-27. <https://tinyurl.com/4bf2zesf>.
- Barrera, Giulia. 2018c. "Protezione dati personali negli archivi. Pubblicate le linee guida dello European Archives Group sull'applicazione del Regolamento europeo protezione dati personali." *Il Mondo degli archivi*. 29 Ottobre 2018. <https://tinyurl.com/5hanzxpj>.
- Barrera, Giulia. 2019. "Protezione dati personali: non è cattiva, è che la disegnano così." *Vediance, notiziario online e open access della Sezione Liguria dell'Associazione Italiana Biblioteche* 29(1). <https://tinyurl.com/3r4wukwm>.
- Bonfiglio-Dosio, Giorgetta. 2023. *Primi passi nel mondo degli archivi. Temi e testi per la formazione archivistica di primo livello*. Padova: CLEUP.
- Carucci, Paola. 2021. "Consultabilità dei documenti e tutela dei dati personali. Tutela del diritto d'autore e di immagine." In *Manuale di archivistica*. A cura di Paola Carucci e Maria Guercio. Roma: Carocci.
- Decreto legislativo 22 gennaio 2004, n. 42, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*.
- Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).
- European Archives Group. 2018. *Guida alla protezione dei dati personali per gli archivi*. Ottobre 2018. <https://tinyurl.com/2x7dvsyb>.
- Garante per la protezione dei dati personali (GPDP). 2018. *Delibera 19 dicembre 2018 n. 531, Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica* (pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101).
- Parlamento, Consiglio e Commissione Europea. 2000. *Carta dei diritti fondamentali dell'Unione europea* (2000/C, 364/01). 18 dicembre 2000. [https://www.europarl.europa.eu/charter/pdf/text\\_it.pdf](https://www.europarl.europa.eu/charter/pdf/text_it.pdf).
- Regolamento UE 2016/679, *Regolamento generale sulla protezione dei dati* (Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).
- Twardzik, Stefano. 2014. "La consultabilità dei documenti." In *Archivistica*. A cura di Linda Giuva e Maria Guercio. Roma: Carocci.