Gianni Penzo Doria[1]

DATA DISPOSAL, RECORDS APPRAISAL

Abstract

In the continuous disciplinary battle between the archival science and the objective of data protection – a controversy nourished exclusively by those who persist in a reductive vision of records management – we are increasingly facing with decisions which will heavily affect a correct way in keeping and preserving the records produced both by public and private producers.

This paper aims to illustrate how a correct vision of archival science is not in conflict with data protection's goal, but rather should be considered to be an integral part of the records creator's point of view.

Keywords: Records Appraisal, Data Protection, Disposal, Data Protection Officer.

SCARTO DI DATI, SELEZIONE DI DOCUMENTI

Sintesi

Nella continua battaglia disciplinare tra archivistica e protezione dei dati personali, alimentata solo da chi persiste in una visione riduttiva della gestione documentale, si assiste – in modo sempre più frequente – a decisioni destinate a incidere pesantemente nella corretta conservazione dei documenti, sia di soggetti pubblici sia di soggetti privati.

L'intervento ha l'obiettivo di illustrare come l'archivistica non sia in contrasto con la protezione dei dati personali, ma deve integrarsi nel soggetto produttore come elemento essenziale

Parole chiave: Selezione, protezione dei dati personali, scarto, responsabile della protezione dei dati.

RAZPOLAGANJE S PODATKI, VREDNOTENJE GRADIVA

V nenehnem boju med področji arhivistike in varovanja podatkov je prišlo do polemike, ki jo ohranjajo izključno tisti, ki vztrajajo pri reduktivni viziji upravljanja z dokumenti. Vse pogosteje se zato soočamo z odločitvami, ki bodo močno vplivale na pravilen način vodenja in ohranjanja zapisov, ki so jih izdelali tako javni kot zasebni producenti.

Namen tega prispevka je ponazoriti, kako pravilna vizija arhivistike ni v nasprotju s ciljem varstva podatkov, temveč bi morala biti obravnavana kot sestavni del stališča ustvarjalca dokumentov.

Ključne besede: *vrednotenje, varstvo podatkov, izločevanje, pooblaščena oseba za varstvo podatkov.*

1 Gianni Penzo Doria, Ph.D., Università degli Studi dell'Insubria, Via Ravasi, 2 – VARESE, e-mail: gianni.penzodoria@gmail.com

1. UNA BATTAGLIA INTERDISCIPLINARE DA EVITARE PER IL BENE DEL SOGGETTO PRODUTTORE

Nella battaglia tra archivistica e protezione dei dati personali, alimentata negli ultimi tempi solo da chi persiste in una visione riduttiva della gestione documentale, si assiste – in modo sempre più frequente – a decisioni unilaterali, che esamineremo *infra*, destinate a incidere pesantemente nella conservazione legale dei documenti, tanto di soggetti pubblici quanto di soggetti privati.

Per tali ragioni, risulta necessario chiarire come l'archivistica non sia in contrasto con la protezione dei dati personali e che, di contro, debba necessariamente maturare l'idea di un'integrazione interdisciplinare a favore del soggetto produttore d'archivio. Si tratta, infatti, di un elemento essenziale della convivenza efficace di due obblighi normativi profondamente differenti e non confliggenti, che devono convivere in un equilibrio istituzionale.

Non a caso, uno dei cardini del GDPR è il rispetto del principio di proporzionalità, come introdotto dal *Considerando* 4: «Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità»[2].

In via preliminare, deve essere precisato che nella letteratura scientifica di settore non esiste una definizione generale di *dato* e di *informazione* in grado di attagliarsi trasversalmente alla protezione dei dati personali, alla scienza dell'informazione, all'archivistica e alla diplomatica.

A questo punto, prima di proseguire nella nostra indagine, risulta opportuno riesaminare le definizioni fondamentali per le nostre discipline, in alcuni casi adagiate comodamente in terre di confine, tenendo comunque presente che a ogni definizione è sotteso, da un lato il rischio della caducità, dall'altro quello della settorialità, che porterebbe ad aumentare il rischio di accezioni ambigue.

Si tratta, infatti, di concetti cosiddetti "primitivi", i quali, in ragione della loro pervasività, non accolgono una serrata necessità definitoria, al pari del concetto di algoritmo (formalizzato per la prima volta da Turing con quella che oggigiorno chiamiamo *macchina di Turing*) e di diversi concetti propri della geometria o delle scienze quantitative. Del resto, anche uno dei testi classici dell'informatica – sul quale si basano le definizioni mutuate da altre discipline – riprende le accezioni da un lessico generalista[3].

2. DATO, INFORMAZIONE E DOCUMENTO

In linea generale, seguendo le indicazioni appena espresse, possiamo affermare che per *dato* si intende un fatto osservabile direttamente o un simbolo non interpretato; per *informazione* si intende un dato o un insieme di dati interpretati in un contesto determinato e significativo; per *conoscenza* si intende un insieme di informazioni organizzate e condivise in un contesto determinato e acquisite attraverso l'apprendimento e l'esperienza.

2 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 (Regolamento generale sulla protezione dei dati - GDPR). Il testo, con un commento sulla trasparenza amministrativa, è stato integralmente pubblicato in questa rivista da (Monteduro 2016). Per una sintesi di raccordo con il Codice privacy, si veda il recente (D'Agostino et al., 2019).

3 Mi riferisco, in particolare, a (Atzeni et al., 2014 5a ed.; 2013). Ne approfitto per ringraziare tre colleghi, Marco Bernardo, Simona Bertè e Franco Cardin, per le preziose indicazioni. Sulla teoria dell'informazione, anche per gli aspetti metodologici, rinvio al fondamentale (Shannon, 1948; 1953). Sulla macchina di Turing, (Cappelli 2008).

Come vedremo tra poco, per parlare di *documento* abbiamo la necessità di introdurre un ulteriore requisito atto a identificarne una rappresentazione formale condivisa tra più domini di conoscenza, cioè l'ontologia in archivistica, in scienza dell'informazione e in protezione dei dati personali.

Nondimeno, per il nostro discorso, non ci può aiutare la manualistica sulla privacy, dal momento che persiste una cristallizzata endiadi di *dato personale* e non di *dato* singolarmente inteso o *tout court*, sulla quale si concentrano tutti i tentativi definitori, perlopiù mutuati dall'ordinamento vigente[4].

Proviamo allora a definire con maggiore compiutezza dato, informazione e documento e, per quanto possibile, in una logica interdisciplinare.

Per *dato* si intende la più piccola unità significativa dell'informazione non ancora elaborata. Ad esempio un dato rappresentato sotto forma di numero potrebbe essere significativo della rappresentazione di una miriade di fatti o fenomeni che soltanto altri dati possono contestualizzare fino a diventare informazione. Infatti, preso singolarmente e in maniera asettica, il numero *301121* potrebbe essere il PIN di una carta di credito, un numero di protocollo oppure, come in questo caso, la data – 30 novembre 2021 – della seconda giornata della *31st Conference "International Archival Day"* dell'*International Institute for the archival science* (Trieste/Italia – Maribor/Slovenia). Pertanto, per comprendere un dato e renderlo significativo, dobbiamo aggregarlo a un altro dato o ad altri dati in grado di determinarne il valore informativo. I dati sono, quindi, materie prime dell'informazione, ma prive di significato specifico, le quali, per ottenerne uno o più di uno, devono subire un'elaborazione[5].

Più rischioso e generalista risulta il concetto di *informazione*, di fatto pervasivo in tutte le discipline umanistiche e nelle scienze dure. Con quel termine, infatti, si intende – in linea generale – un insieme di dati aggregati che possono essere comunicati nel tempo e nello spazio[6].

Quando un dato si affianca a un altro dato per determinarne un significato si parla di *metadato* (dal greco "meta", con il significato di *sopra*, cioè di *dato sul dato*). Per esempio, se prendiamo il dato *301121* e lo affianchiamo a un dato descrittivo della seconda giornata della *31st Conference*, potremmo ottenere una sequenza del genere:

<date2_conference_IIAS2021> 301121 <\date2_conference_IIAS2021>

Questi dati aggregati valorizzano una o più informazioni, ossia – nel caso in commento – il contenuto informativo riferito alla data della seconda giornata dello IIAS 2021, la quale risulta esattamente il 30 novembre 2021 (Vivarelli, 2004).

Come conseguenza di quanto esposto finora, possiamo affermare che sussiste un'interdipendenza monodirezionale tra dato e informazione. Infatti, mentre l'informazione discende dai dati e dalla loro valorizzazione prodotta da altri dati anche indipendenti tra loro, i dati non dipendono in alcun modo dall'informazione.

Per *documento* – in senso generale e non archivistico – si intende una o più informazioni affisse stabilmente su un qualsiasi tipo di supporto. In altre parole, qualsiasi contenuto

4 Si vedano, ex multis, le pubblicazioni importanti e poderose come (AA.VV. 2019), fino al recentissimo (Codice della Privacy 2021).

5 «Data is an individual unit that contains raw materials which do not carry any specific meaning», così Cambridge International, AS & A Level Information Technology, https://www.cambridgeinternational.org/images/285017-data-information-and-knowledge.pdf (verificato il 21 novembre 2021).

6 Sull'ambiguità del concetto di informazione e per la copiosa rassegna bibliografica interdisciplinare, Riccardo Ridi, La piramide dell'informazione: una introduzione, https://aibstudi.aib.it/article/view/11903/11481 (verificato il 21 novembre 2021).

informativo, se affisso in un supporto, può essere considerato un documento. Non a caso, nell'ambito ordinamentale europeo del digitale, come stabilito dal regolamento eIDAS, la definizione di documento elettronico è la seguente: «qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva»[7].

Per *documento archivistico*, inoltre, seguendo la definizione del vocabolario IIAS (*documento – unità informativa)* e del glossario di InterPares parzialmente rielaborato, si intende un documento prodotto da un soggetto come strumento e residuo della propria attività pratica[8].

A questo punto, non possiamo tralasciare che, in ambito archivistico, la rappresentazione di un documento digitale non pertiene a una dimensione statica, ma a una soluzione pluridimensionale in cui diverse componenti – sotto forma di dati e di metadati – si aggregano in un susseguirsi di operazioni tecniche e di contesto (non soltanto di vincolo archivistico), che richiedono una grande preparazione professionale, a pena di perdita della memoria o di parti significative della memoria stessa, le quali – anche in minima parte – finirebbero con il compromettere uno degli elementi imprescindibili per l'ambito diplomatistico: l'autenticità.

Infatti, la «rappresentazione di un documento non è altro che il risultato dell'aggregazione istantanea di componenti digitali distinte all'origine, come banalmente esemplificato da una qualunque pagina web; e sempre più spesso i sistemi documentari digitali sono purtroppo strutturati in maniera drammaticamente puntiforme, immergendo i documenti all'interno di depositi pressoché privi di organizzazione e dimenticando che gran parte del significato degli oggetti risiede proprio nelle relazioni cui partecipano, come risulta evidente – ad esempio – dal ruolo essenziale che l'organizzazione gerarchica di un archivio assume per la comprensione delle sue carte» (Michetti, 2008, pp. 33).

Un'ultima precisazione lessicale utile al nostro discorso è la definizione di *dato personale*. Seguendo l'ordinamento positivo e, nella fattispecie, ai sensi dell'art. 4 del *General Data Protection Regulation* – GDPR, per dato personale si intende «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

In buona sostanza, un dato con l'aggiunta dell'aggettivo *personale* diventa informazione giuridicamente rilevante.

3. I DOCUMENTI PUBBLICI CONTENGONO IN RE IPSA DATI PERSONALI

A questo punto si impone un corollario importante per tutte le definizioni esposte finora. Le amministrazioni pubbliche trattano costantemente dati personali dei propri cittadini, degli utenti dei propri servizi e, ovviamente, dei titolari di poteri di firma, dei soggetti istruttori e dei responsabili dei procedimenti amministrativi e di tutto il personale interno.

7 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE: eIDAS è acronimo di electronic IDentification, Authentication and trust Services.

8 Il vocabolario multilingue dello IIAS si trova a seguente link http://www.iias-trieste-maribor.eu/attivita-2/dizionario-plurilingue-2/dizionario/ (verificato il 21 novembre 2021) e quello di InterPares si trova già nei primi risultati di IP1, datato al dicembre 2001 al seguente link http://interpares.org/. Poi si veda (Duranti, 1997, pp. 15). La definizione proposta era di «documento prodotto o ricevuto da una persona fisica o giuridica come strumento e residuo della propria attività pratica». Per quanto attiene alla diplomatica, la definizione si trova in (Duranti, 1989).

Nella teoria generale del diritto amministrativo, infatti, uno dei casi di nullità più rilevanti è rappresentato dalla mancanza di un soggetto cui attribuire un atto amministrativo e, nel rispetto del diritto positivo, ogni documento pubblico uscito da una cancelleria pubblica deve contenere anche il nominativo del responsabile dell'istruttoria e, nella maggioranza dei casi, anche del destinatario di un provvedimento determinato.

Contestualizzato tutto ciò all'ambito diplomatistico, possiamo affermare che *auctor* e *scriptor* sono sempre presenti, così come la *mansio* risulta pressoché sempre presente. Infatti, anche nei documenti interni, ad es. verbali, deliberazioni, determinazioni, ordinanze, etc., compaiono sempre altri dati personali, riferiti ai partecipanti a una collegialità amministrativa, al destinatario di un provvedimento restrittivo e così via.

Da ciò consegue che, per perseguire finalità di pubblico interesse, nei documenti amministrativi prodotti dalle amministrazioni pubbliche è di fatto impossibile evitare il trattamento di dati personali con persistenza nel tempo.

Il problema – sempre ammesso, come vedremo, che di problema si tratti – è che i dati personali sono memorizzati all'interno di uno o più sistemi informatici, e, contemporaneamente, conservati in fondi differenti in quanto elementi di documenti amministrativi. Non a caso, memorizzazione di dati e conservazione di documenti rappresentano funzioni distinte per le amministrazioni pubbliche, ma perfettamente integrabili.

Facciamo qualche esempio. In un Comune i dati personali di un cittadino sono conservati nel database dello Stato civile, mentre i documenti inerenti al medesimo cittadino sono conservati nel fondo dello Stato civile, sia in fascicoli nominativi, sia nel Registro degli atti dello Stato civile. La carriera universitaria contenente anche i dati personali di uno studente – a volte anche cd. "sensibili", ad es. in caso di disabilità o di disturbi dell'apprendimento – è memorizzata nel sistema informatico gestionale, al pari dei dati inerenti agli esami sostenuti, mentre i documenti di riferimento, anche sotto forma di registro degli esami sostenuti o di certificazioni inerenti allo stato di salute, sono conservati come documenti amministrativi autonomi nel fascicolo di studente e nel fondo della Segreteria studenti o della Segreteria didattica[9].

Anche sul fronte dell'albo on-line ci sono numerosi documenti contenenti dati personali soggetti ad anonimizzazione tramite la corruzione di una copia in autotutela. Sul punto, anche con finalità di pubblicità legale, è intervenuto tempestivamente il Garante per la protezione dei dati personali, proprio per definire i confini del trattamento da parte delle amministrazioni pubbliche[10].

9 Il GDPR non utilizza il termine "sensibili", bensì "appartenenti a categorie particolari" (art. 9). L'endiadi dati sensibili era contenuta nelle definizioni del D.Lgs. 196/2003, art. 4, comma 1, lett. d): «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». A margine, visto che l'argomento principale è racchiuso nel GDPR, è comunque opportuno rilevare che il D.Lgs. 196/2003 dedica tutto il Titolo VII al Trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (artt. 97-110bis).

10 Garante per la protezione dei dati personali, Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web, Deliberazione 2 marzo 2011, n. 88. Sul punto, cfr. B. Montini, G. Penzo Doria, Albo on-line e privacy: commento alla Deliberazione del Garante 2 marzo 2011, n. 88, https://www.filodiritto.com/albo-line-e-privacy-commento-alla-deliberazione-del-garante-2-marzo-2011-n-88 (verificato il 21 novembre 2021). A seguito dell'emanazione del D.Lgs. 33/2013 (per il quale v. infra nota 22), sono state sostituite dal Garante per la protezione dei dati personali con deliberazione 15 maggio 2014, n. 243, Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.

Come abbiamo potuto evidenziare, dunque, per le amministrazioni pubbliche il trattamento dei dati personali è pervasivo e non risparmia di fatto alcun documento amministrativo.

4. DATA RETENTION E RECORDS RETENTION

Orbene, uno dei pilastri fondanti dell'ordinamento giuridico sulla protezione dei dati personali è il tempo di conservazione (*Data retention*), come definito dall'art. 5, paragrafo 1, lett. e) del GDPR in merito ai principi applicabili al trattamento di dati personali. Tali dati, infatti, 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, 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 («limitazione della conservazione»)».

Anche gli archivi non sono soggetti a conservazione indeterminata e, in perfetta simmetria, esiste il concetto di tempo di conservazione dei documenti (*Records retention)*. Esso è orientato non soltanto alle finalità inerenti all'utilizzo, ma anche al valore storico che gli archivi possiedono fin dall'origine, cioè all'atto della produzione.

I tempi di conservazione, infatti, sono descritti in strumenti altamente professionali chiamati Massimari di selezione (o Piani di conservazione – *Retention plans*) e rispondono a logiche rivolte non soltanto – come nel caso dei dati personali – alla tutela dell'individuo, ma anche alla conservazione della memoria di un soggetto produttore come funzione sociale per la collettività.

Il titolo di questo saggio, in aderenza al lessico tecnico di protezione dei dati personali e di archivistica, avrebbe potuto essere *Cancellazione di dati, selezione di documenti (Data erasure, Records appraisal)*. Per mantenere un lessico archivistico omogeneo, invece, si è preferito quello di *Scarto di dati, selezione di documenti (Data disposal, Records appraisal)*.

Il GDPR, infatti, non conosce il termine *scarto (disposal)*, ma esclusivamente *cancellazione (erasure)*. Sono invece quasi irrilevanti per il nostro discorso altri termini del GDPR, come *distruzione (destruction)* o *danno (damage)*. Anzi, per simmetria con le disposizioni del GDPR, la cancellazione di dati è concettualmente assimilabile al *diritto all'oblio* o, per rimanere alla traduzione letterale, *diritto di essere dimenticati (Right to be forgotten)*, che esamineremo a breve proprio per tentare di equilibrare due esigenze apparentemente opposte: la cancellazione di dati e la conservazione di documenti.

Tuttavia, già nell'art. 5 del GDPR richiamato *supra*, è inserita anche la soluzione per la conservazione di dati sotto forma di documenti per necessità delle amministrazioni pubbliche, con un richiamo al successivo art. 89 sulle finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Invece, assistiamo sempre più frequentemente a posizioni intransigenti e verticali da parte del Responsabile della protezione dei dati personali (*Data Protection Officer – DPO*), il quale ordina la distruzione di documenti contenenti dati personali non appena spirato il termine inerente alle finalità del trattamento. In questo caso, il passaggio all'ordine di distruzione di tutti i documenti che contengono dati personali, per azzerare il rischio di conservarli oltre il termine, è spesso breve.

Prima di proporre una soluzione possibile, vediamo di chiarire i contorni della figura del DPO, come introdotta nell'ordinamento europeo dall'art. 37 del GDPR. Il professionista dei dati, innanzitutto, deve assolvere ai compiti previsti dal successivo art. 39. In parti-

colare, si tratta di un ruolo strategico di consulenza trasversale, di analisi e di sorveglianza sull'applicazione della normativa vigente in materia[11].

Trasversale, dicevamo. Uno dei problemi più evidenti è che in alcune amministrazioni pubbliche operano DPO privi di preparazione archivistica, a volte claudicanti nel diritto e spogliati di quel bagaglio imprescindibile di conoscenza tecniche (e non tecnologiche) atto a sistematizzare e a contestualizzare l'applicazione della protezione dei dati personali ai documenti pubblici. In larga misura sono operatori di informatica, non scienziati dell'informazione.

Quando il ruolo di DPO è ricoperto da una figura del genere, poco avvezza all'analisi di sistemi e alla *cybersecurity*, ma dedito a operazioni più consone all'informatica individuale, il quadro è completo[12].

Per quanto riguarda la conservazione dei documenti archivistici che – pressoché inevitabilmente – contengono dati personali, il legislatore europeo ha introdotto due *Considerandi*. In particolare, il C50 dispone che: «Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile»[13].

Un altro *Considerando* molto importante è il C158, anche per gli aspetti sociali e di evidenza probatoria contro la *post-verità* e verso un'educazione civica archivistica e digitale. Ecco, dunque, il dettato normativo europeo del C158: «Qualora i dati personali siano trattati a fini di archiviazione, il presente regolamento dovrebbe applicarsi anche a tale tipo di trattamento, tenendo presente che non dovrebbe applicarsi ai dati delle persone decedute. Le autorità pubbliche o gli organismi pubblici o privati che tengono registri [traduzione corretta: documenti archivistici] di interesse pubblico dovrebbero essere servizi che, in virtù del diritto dell'Unione o degli Stati membri, hanno l'obbligo legale di acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a registri [traduzione corretta: documenti archivis-

11 GDPR, art. 39: «a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'autorità di controllo; e e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione».

12 Sul punto, non sorprenda la questione, dal momento che – semplicemente a scorrere i bandi pubblici per la manifestazione di interesse a ricoprire il ruolo di DPO – l'offerta economica si aggira intorno ai 2-3.000 euro lordi, compenso del tutto inadeguato per un professionista dei dati, probabilmente più consono a una figura avvezza alle operazioni pratiche sugli applicativi più diffusi. E la protezione dei dati personali sarà esponenzialmente sempre più legata alla sicurezza informatica, al punto da poter individuare una figura di privacycybersecurity officer.

13 GDPR, C50: «If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations».

tici] con un valore a lungo termine per l'interesse pubblico generale. Gli Stati membri dovrebbero inoltre essere autorizzati a prevedere il trattamento ulteriore dei dati personali per finalità di archiviazione, per esempio al fine di fornire specifiche informazioni connesse al comportamento politico sotto precedenti regimi statali totalitari, a genocidi, crimini contro l'umanità, in particolare l'Olocausto, o crimini di guerra».

In poche parole, per finalità archivistiche – che il legislatore enuclea come pubblico interesse, ricerca scientifica, storica o statistica – il trattamento è lecito e compatibile, laddove per *trattamento* si intende anche la conservazione di documenti archivistici. Infatti, l'art. 4, punto 2, del GDPR intende per 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»[14].

Non bastasse, il legislatore europeo ha ribadito il concetto anche nel C65, secondo capoverso: «Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria»[15].

5. DUE CASI CONCRETI

Da quanto finora illustrato, dovrebbe essere evidente, anche al più impreparato dei DPO, che la conservazione dei documenti archivistici risponde ai criteri di selezione documentale e non di cancellazione di dati personali.

Per queste ragioni è inaccettabile trovare nelle amministrazioni pubbliche un ordine di servizio come il seguente (qui anonimizzato): «Al fine di prevenire il più possibile accessi abusivi alle informazioni contenenti dati personali, soprattutto in presenza di dati c.d. particolari (come quelli relativi allo stato di salute dei cittadini con disabilità), sono state predisposte le seguenti istruzioni operative per la distruzione dei documenti cartacei. Tale procedura di smaltimento prevede, in particolare, l'utilizzo di distruggi-documenti prima che questi ultimi vengano cestinati».

Al di là del lessico incerto e delle omissioni riguardo alle autorizzazioni necessarie, giova ribadire che le procedure di scarto, cioè di eliminazione legale di documenti, rispondono all'art. 21, comma 1, lett. d) del D.Lgs. 42/2004 e necessitano di autorizzazione preventiva da parte del Ministero della Cultura. Tale autorizzazione è rilasciata attra-

14 GDPR, art. 4: « 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction». Qui, rispetto all'ordinamento italiano previgente (675/1996) si evidenzia l'opportuna precisazione che il concetto di trattamento si applica anche ai dati non presenti in database.

15 GDPR, C65: «However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims».

verso la Soprintendenza archivistica e bibliografica competente per territorio per gli archivi degli enti pubblici e quelli privati dichiarati di interesse culturale e attraverso la Commissione di sorveglianza per gli archivi statali[16].

Un secondo caso è stato oggetto di discussione in un gruppo di lavoro interprofessionale universitario. La richiesta del laureato, inviata attraverso la posta elettronica priva di identificazione, era la seguente: «Chiedo la cancellazione dei miei dati personali da tutte le banche dati, archivi e registri dell'università fatta eccezione per quelli contenuti in atti che devono essere obbligatoriamente conservati». Due operatori di informatica rispondono prospettando due casi, con la seconda risposta davvero imbarazzante:

a) il fascicolo di studente è gestito interamente in digitale e inviato in conservazione, questo potrebbe giustificare la cancellazione completa di tutti i dati dal database del gestionale carriere studenti mantenendo solo il fascicolo;

b) il fascicolo elettronico è da sempre incompleto e non è mai stato inviato in conservazione, i dati di carriera sono nel gestionale, ovviamente non si possono cancellare, a meno di non copiare tutto sui documenti nel fascicolo di studente.

Inoltre, in alcune circostanze i DPO agitano le sanzioni previste dal GDPR, che li spingono a fare pressioni sul titolare del trattamento. Ai DPO, oltre alle sanzioni previste dal D.Lgs. 42/2004, giova ricordare che, oltre alle sanzioni previste dal D.Lgs. 42/2004, l'art. 490 del Codice penale, come modificato dal DLgs. 7/2016, sulla distruzione dei documenti archivistici dispone quanto segue: «Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477 e 482, secondo le distinzioni in essi contenute». Non si scherza, dunque, con le sanzioni previste per la distruzione di documenti pubblici, con pene che variano da uno a dieci anni[17].

Del resto, la normativa di settore sugli archivi aveva con chiarezza messo dei limiti invalicabili all'impulso sfrenato di distruggere avalutativamente i dati contenuti in documenti archivistici. Infatti, lo stesso D.Lgs. 42/2004, all'art. 126, comma 3, aveva chiaramente stabilito che «La consultazione per scopi storici dei documenti contenenti dati personali è assoggettata anche alle disposizioni del codice di deontologia e di buona condotta previsto dalla normativa in materia di trattamento dei dati personali».

Tale previsione – e qui non è ammessa alcuna ignoranza da parte dei DPO operatori di informatica – oggi trova la sua applicazione più concreta nelle regole deontologiche approvate tanto dal Garante privacy quanto, più recentemente, dal Ministero della giustizia[18].

16 D.Lgs. 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137, con particolare riferimento all'art. 21, comma 1, lett. d), sono subordinati all'autorizzazione del Ministero: «lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13 , nonché lo scarto di materiale bibliografico delle biblioteche pubbliche, con l'eccezione prevista all'articolo 10, comma 2, lettera c), e delle biblioteche private per le quali sia intervenuta la dichiarazione ai sensi dell'articolo 13». Per gli archivi statali, le Commissione di sorveglianza sono tuttora regolate dal DPR 8 gennaio 2001, n. 37, Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato (n. 42, allegato 1, della legge n. 50/1999).

17 Limpidamente, ne aveva trattato più di sessant'anni fa (Olla Repetto, 1960).

18 Garante per la protezione dei dati, Deliberazione 19 dicembre 2018, n. 513, 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 e Ministero della giustizia, Decreto, 15 marzo 2019, Inserimento nell'allegato A del decreto legislativo 30 giugno 2003, n. 196, delle regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica.

Per chiudere il cerchio su questo discorso, rimane soltanto da ricordare che stanno sviluppandosi nuovi mestieri di intermediari dei dati – detti anche *Data Broker* – con il compito di aiutare cittadini e imprese a destreggiarsi tra i dati legittimamente trattati dalle amministrazioni pubbliche. Il fenomeno – distinto da quello dei *Data Reseller*, veri e propri cacciatori di dati – è attualmente all'attenzione del Garante per la protezione dei dati personali.

6. UN PONTE VERSO I DPO: IL GRUPPO ARCHIVI EUROPEO

Uno dei documenti più importanti pensato e redatto per coniugare le esigenze di archivistica e di protezione dei dati personali è rappresentato dalle *Linee guida sull'applicazione del Regolamento europeo di protezione dati personali negli archivi*, elaborate dal Gruppo Archivi Europei (*European Archives Group* – EAG)[19].

Il documento rappresenta una sorta di vademecum pensato appositamente per gli archivisti nell'applicazione di una norma con sanzioni assai severe, sia in ambito amministrativo sia in ambito penale, cercando correttamente di destrutturare ogni paura. Del resto, lo EAG è un gruppo ufficiale di esperti della Commissione europea, istituito agli inizi del 2006 e formato da rappresentanti degli archivi nazionali dei paesi membri dell'UE, che ha seguito la genesi del GDPR dal 2012 al 2016.

Gli archivisti, infatti, non sono votati alla conservazione passiva, né indiscriminata, né a oltranza. Anzi, una delle funzioni più delicate della funzione archivistica è proprio la selezione, mediante valutazione, della necessità di conservazione di documenti determinati. Proprio a questo servono i massimari di selezione (*Retention plans*)[20].

Per tali ragioni, il documento di EAG, richiamando l'aderenza all'art. 25 del GDPR della conservazione dei documenti archivistici, afferma con forza le attività di presidio che i servizi archivistici devono porre in essere: «Archive services adopt an appraisal policy that limits the permanent preservation of records containing personal data to what is really necessary, according to their mission. They put into practice Article 25 by carefully drafting retention plans that define which kind of files containing personal data have to be selected for permanent preservation. For archive services, retention plans are tools to demonstrate compliance with Article 25» (pp. 23).

Infine, a mettere una pietra tombale sulle ingerenze inappropriate dei DPO sulla conservazione dei documenti archivistici interviene l'art. 89 del GDPR, con linearità cristallina:

art. 89
Garanzie e deroghe relative al trattamento a fini di archiviazione
nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudoanonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano

19 La notizia è stata data opportunamente dalla referente italiana, Giulia Barrera, su «Il Mondo degli archivi», 29 ottobre 2018: http://www.ilmondodegliarchivi.org/rubriche/in-italia/685-protezione-dati-personali-negli-archivi-pubblicate-le-linee-guida-dello-european-archives-group-sull-applicazione-del-regolamento-europeo-protezione-dati-personali-gdpr. La pagina di riferimento istituzionale dell'EAG è la seguente: https://ec.europa.eu/info/about-european-commission/service-standards-and-principles/transparency/freedom-information/access-documents/information-and-document-management/archival-policy/european-archives-group_en.

20 Sul tema resta ancora valido, per gli aspetti generali e metodologici, (Duranti, 1994), mentre è doveroso citare lo studio antesignano di (Naugler, 1983) e il commento di (Cox, 1990).

essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

Anche l'EAG interviene con chiarezza distinguendo tra il tempo di conservazione di dati e il tempo di conservazione di documenti. Ecco la traduzione di un passaggio importante (il sottolineato è presente nell'originale): «Attenzione: Dal punto di vista dei servizi archivistici, è di particolare importanza far presente ai soggetti produttori che il "tempo di conservazione" non deve essere confuso con lo "smaltimento" delle informazioni e che dovrebbero agire in conformità con la legge sugli archivi e secondo quanto previsto dai massimari di scarto. I dati archiviati nell'interesse pubblico, infatti, non devono mai essere distrutti»[21].

In altre parole, non essendo il diritto alla protezione dei dati personali assoluto, una compressione limitata di quel diritto per finalità di pubblico interesse e di sicurezza pubblica è ampiamente giustificata, prima di tutto dal buon senso e, in seconda battuta, dalle norme positive.

7. IL DIRITTO DI ACCESSO E LA PROTEZIONE DEI DATI PERSONALI

In caso di opposizione di un controinteressato all'esercizio del diritto di accesso da parte di terzi, non è possibile esporre la condizione o la preoccupazione che un documento determinato contenga dati personali del controinteressato medesimo. Infatti, proprio in ossequio a quanto previsto dall'ordinamento vigente, le norme di riferimento restano la legge 241/1990 per l'accesso documentale e il D.Lgs. 33/2013 per l'accesso civico[22].

Su questo tema specifico il Codice privacy è lapidario[23].

21 Testo originale: «Attention: From the point of view of archive services, it is of particular importance to point out to archives' creators that 'retention period' must not be confused with 'disposal' of information, and that they should act in conformity with the Law on Archives and as stipulated in the archival disposal schedules. Data archived in the public interest must indeed never be destroyed».

22 Legge 7 agosto 1990, n. 241, Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi e D.Lgs. 14 marzo 2013, n. 33, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.

23 D.Lgs. 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. Il titolo è stato così modificato dall'art. 1, comma 1, D.Lgs. 10 agosto 2018, n. 101. Il titolo originario, meno esteso, era infatti Codice in materia di protezione dei dati personali.

Infatti, all'art. 59 (Accesso a documenti amministrativi e accesso civico), il D.Lgs. 196/2003, ordina che: «1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati di cui agli articoli 9 e 10 del regolamento e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso.

1-bis. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33».

8. CONCLUSIONI

La selezione dei documenti contenenti (anche) dati personali risponde alle procedure e alle norme archivistiche e, più in generale, a quelle sull'attività amministrativa. Anche l'esercizio del diritto di accesso a documenti contenenti dati personali sfugge correttamente alla sfera di competenza del GDPR e rimane in capo all'ordinamento in materia di diritto di accesso e, più in generale, di trasparenza amministrativa.

A questo punto, risulta necessario rafforzare la consapevolezza del ruolo degli archivi nelle amministrazioni pubbliche e nelle aziende private, in una visione non subalterna rispetto alla protezione dei dati personali. In particolare, è necessario rendere partecipi i DPO del valore degli archivi pubblici senza ambiguità o subordine rispetto alla privacy e che, sul punto, la gestione documentale deve necessariamente intersecarsi con la protezione dei dati personali in una visione interdisciplinare.

Al riguardo, le recenti Linee guida AgID sul documento informatico, tra i principi generali della gestione documentale descritti al § 1.11, dispongono che «il sistema di gestione informatico dei documenti, la cui tenuta può anche essere delegata a terzi, affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio»[24].

In quest'ambito archivistico e digitale, la protezione dei dati personali è citata più volte, con contezza sia per gli aspetti conservativi, sia per gli aspetti di sicurezza informatica, spesso unitamente al Responsabile della transizione digitale, altra figura imprescindibile per l'amministrazione pubblica italiana. Ciò testimonia la necessità di agire trasversalmente sul fronte di una funzione delicatissima inerente alla tutela di un bene della vita come sono gli archivi pubblici[25].

24 Agenzia per l'Italia digitale, Determinazione del Direttore Generale 17 maggio 2021, n. 371, Linee guida sulla formazione, gestione e conservazione dei documenti informatici, con la quale è stata modifica e integrata la precedente determinazione 9 settembre 2020, n. 407 ed è stata differita l'entrata in vigore dal 7 giugno 2021 al 1° gennaio 2022.

25 Le Linee guida trattano la protezione dei dati personali, ad. es., ai §§ 2.1.1, 3.1.6, 3.4, 3.5, 3.9, 4.1, 4.5, 4.9, 4.10, 4.11. Sulla funzione cruciale dell'archivio anche di bene immateriale, cfr. (Penzo Doria 2008).

REFERENCE LIST

Alagna, I. M., Bolognini, L., Capparelli, F., Carpenelli, M. E., Cristofari, G., D' Ottavio, A., Fiaschi, A., Grieco, L., Macinati, A., Marchese, M., Pavese, V. M., Pelino, E., Policella, E., Rossi, C. C., Sartore, F., Toma, A., Zipponi, S. (2019). *Codice della disciplina della Privacy*. Milano, Giuffrè.

Atzeni, P., Ceri, S., Fraternali, P., Paraboschi, S., Torlone, R. (2013). *Basi di dati: modelli e linguaggi di interrogazione*. Milano, McGraw-Hill Italia.

Atzeni, P., Ceri, S., Fraternali, P., Paraboschi, S., Torlone, R. (2014). *Basi di dati*, Milano, McGraw-Hill Italia.

Cappelli, M. (2008). *Enciclopedia della Scienza e della Tecnica*, Roma, Istituto dell'Enciclopedia Treccani, s.v.

R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (eds.). (2021). *Codice della Privacy e Data Protection* Milano, Giuffrè.

Cox, R. J. (1990). RAMP Studies and Related UNESCO Publications: An International Source for Archival Administration. *The American Archivist, 53*(3), 488–495.

D'Agostino A., Barlassina L. R., Colarocco, V. (2019). *Commentario al Regolamento UE 2006/679 e al Codice privacy aggiornato*, Milano, Top Legal Academy.

Duranti, L. (1989). Diplomatics. New Uses for an Old Science, Part 1. *Archivaria, 28*. 7–27. , poi tutti gli articoli rielaborati sono ora contenuti in Ead. (1998). *Diplomatics. New Uses for an Old Science*, Scarecrow Press.

Duranti, L. (1994). The Concept of Appraisal and Archival Theory. *American Archivist, 57*(2). 328–344.

Duranti, L. (1997). *I documenti archivistici. La gestione dell'archivio da parte dell'ente produttore.* Roma, Ministero per i beni culturali e ambientali – Ufficio centrale per i beni archivistici.

Michetti, G. (2008). Il modello OAIS. *DigItalia. Rivista del digitale nei beni culturali, III*(1). 32–49.

Monteduro, F. (2016). Fra GDPR europeo e FOIA italiano: nuovi regolamenti sulla protezione dei dati ed il diritto all'accesso. *Atlanti, 26*(1), 137–176.

Naugler, H. (1983). *The archival appraisal of machine-readable records: a RAMP study with guidelines*. Parigi, UNESCO.

Olla Repetto, G. (1960). Conseguenze penali della illecita eliminazione dei documenti. *Rassegna degli Archivi di Stato, XX*, 235–249.

Penzo Doria, G. (2008). L'archivio come bene della vita. *Scrinia. Rivista di archivistica, paleografia e diplomatica e scienze storiche*, *V*(1-3), 21–37.

Shannon, C. E. (1948). A mathematical theory of communication.*The Bell system technical journal, 27* (July/October), 379–423, 623–656.

Shannon, C. E. (1953). The lattice theory of information. *Transactions of the IRE professional group on information theory, 1*, 105–107.

Vivarelli, M. (2004). Alcune considerazioni sugli usi del termine "informazione". *Culture del testo e del documento, 5*, 19–65.

Typology: 1.01 Original scientific research