

Protezione dati personali: non è cattiva, è che la disegnano così¹

Giulia Barrera

Il Regolamento UE 2016/679 sulla protezione dei personali¹ gode di cattiva fama. Ci siamo spazientiti quando, alla sua entrata in vigore, siamo stati inondati di messaggi che ci chiedevano di autorizzare il trattamento dei nostri dati, per continuare a ricevere newsletter. L'insofferenza è andata crescendo nei mesi successivi, quando a ogni passo della nostra navigazione in internet ci siamo trovati ad autorizzare l'invio di cookies e il trattamento dei nostri dati, senza avere in realtà idea di cosa ne faranno i siti che autorizziamo. Fra molti cittadini serpeggia il sospetto che il Regolamento abbia prodotto tanta burocrazia in più, con pochi benefici effettivi e ben si presti, dunque, a rafforzare gli stereotipi negativi rispetto all'operato dell'Unione Europea.

Fra gli archivisti, il Regolamento europeo sulla protezione dei personali (d'ora innanzi GDPR) gode di fama ancor peggiore: la protezione dati personali sembra andare in rotta di collisione con la conservazione archivistica. In molti uffici pubblici e privati, le salatissime sanzioni previste dal GDPR – che possono arrivare fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale (art. 83) – hanno seminato il terrore, con conseguente corsa allo scarto dei documenti contenenti dati personali. Fra il rischio di violare il codice dei beni culturali e quello di violare il GDPR, è facile intuire cosa scelgono i dirigenti di enti pubblici e privati. Così, gli archivisti si sentono più che mai soli e incompresi, a combattere con armi impari la loro battaglia per la conservazione delle fonti per la ricerca storica e per garantire i diritti dei cittadini.

Ma è proprio vero che il GDPR è nemico della conservazione archivistica? E siamo proprio sicuri che il GDPR serva solo alla proliferazione di liberatorie da firmare a ogni piè sospinto?

Certamente il GDPR ha limiti e difetti, ma al momento attuale è la norma migliore che sia stata prodotta a livello internazionale per proteggere i cittadini dallo strapotere dei giganti del web e dall'uso spregiudicato dei dati personali da parte di altri potentati pubblici e privati.

Solo da poco, noi semplici cittadini abbiamo iniziato a renderci conto di quanto i dati personali siano uno strumento per accumulare ricchezza e potere. Si parla ormai sempre più spesso dei dati personali come del "nuovo petrolio"². E come il controllo del petrolio è stato causa di conflitti senza esclusione di colpi, così oggi iniziamo a vedere analoghi conflitti per il controllo dei dati. Nel discorso di presentazione della relazione sull'attività dell'Autorità garante per la protezione dati personali nel 2018, Antonello Soro ha ricordato che

Lo stesso antagonismo commerciale tra USA e Cina sottende una competizione per l'egemonia tecnologica, che disegna la nuova geografia del potere planetario. Il possesso e lo sfruttamento dei dati, che si accumulano nell'infosfera, sono la posta in palio.³

Il controllo dei dati personali può essere un formidabile strumento di potere di pochi su molti. In gioco sono niente di meno che la democrazia e la libertà individuale.

Per questo l'Unione Europea ha posto la protezione dei dati di carattere personale fra i diritti protetti dalla propria Carta dei diritti fondamentali, nell'ambito del titolo II: *Libertà* (art. 8):

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. (...)

Questo non vuol dire che per la UE la protezione dei dati personali venga prima di ogni altra cosa. Nell'ambito dello stesso titolo II, si trovano, con pari dignità, l'articolo relativo alla libertà d'informazione, che include la libertà di ricevere informazioni e quindi la ricerca d'archivio (art. 11), e l'articolo che tutela la libertà delle arti e delle scienze e quindi anche la ricerca storica (art. 14). La protezione dei dati personali deve inoltre essere bilanciata con altre esigenze, come la tutela della sicurezza dei cittadini o la tutela della salute pubblica. Il GDPR bilancia questi diversi diritti prevedendo numerose deroghe agli obblighi e ai divieti relativi al trattamento dei dati personali. In alcuni casi, le deroghe sono normate dal regolamento stesso, in altri casi viene accordata ai legislatori nazionali la facoltà di introdurre deroghe. L'art. 89 permette, nel caso di trattamenti a fini di "archiviazione nel pubblico interesse", che la legislazione nazionale introduca deroghe – pur nell'ambito di parametri ben definiti – alle disposizioni di ben sei articoli del GDPR.

Per quanto riguarda le questioni più cruciali per gli archivisti – ovvero la possibilità stessa di conservare i documenti contenenti dati personali – le deroghe sono previste dal GDPR stesso, che prevede come principio generale che i dati personali siano conservati solo per il tempo necessario a conseguire le finalità del trattamento (principio della "limitazione della conservazione"), ma subito aggiunge che possono essere conservati più a lungo "a fini di archiviazione nel pubblico interesse" (art. 5, c. 1, lett. c). Il GDPR afferma inoltre il diritto delle persone ad ottenere la cancellazione dei dati che le riguardano, ma prevede che tale diritto non si applichi nel caso di archiviazione nel pubblico interesse (art. 17).

I principi applicabili al trattamento dei dati personali previsti dal GDPR (art. 5) in realtà non sono una novità, in quanto erano già previsti dalla direttiva europea 95/46/CE sulla protezione dei dati personali e dalle legislazioni nazionali emanate in sua applicazione⁴, che in buona misura prevedevano anche i diritti che il GDPR riconosce agli interessati (cioè alle persone a cui si riferiscono i dati). Ad esempio, il diritto di rettifica (art. 16) già esisteva ed il legislatore italiano aveva trovato il modo di renderlo compatibile con la conservazione archivistica: il *Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici* prevedeva infatti che:

1. L'archivista favorisce l'esercizio del diritto degli interessati alla rettifica o all'integrazione dei dati, garantendone la conservazione secon-

do modalità che assicurino la distinzione delle fonti originarie dalla documentazione successivamente acquisita. (art. 7)

Il *Codice di deontologia* è stato ritoccato per renderlo compatibile con il GDPR e ribattezzato *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica*⁵; questo articolo è rimasto così com'era, così come la maggior parte degli altri articoli.

Ma allora cosa ha cambiato il GDPR? Tanto rumore per nulla? Le novità ci sono e sono sostanziali. Inoltre è cambiato il contesto in cui si inserisce la norma: abbiamo tutti la sensazione che si debba applicare la protezione dei dati personali più rigorosamente di prima non solo perché ci sono sanzioni più severe, ma anche perché è assai più probabile che i cittadini ci chiedano conto di come trattiamo i loro dati. Non è detto che ciò sia negativo per gli archivi.

Forse la principale innovazione del GDPR rispetto alla direttiva del 1995 è una maggiore responsabilizzazione del titolare del trattamento: al titolare è chiesto di operare in modo che il trattamento limiti il più possibile i rischi per le libertà e i diritti degli interessati. Questo significa che non è sufficiente qualche adempimento formale per "mettersi in regola" con il GDPR. Bisogna guardare alla sostanza, al fine di trovare la soluzione più idonea. E bisogna farlo sin dal momento in cui si imposta un nuovo trattamento (art. 25 *Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*): ad esempio, al momento in cui si progetta un software per la gestione informatica della sala di studio o un sistema informativo di descrizione archivistica.

Il GDPR indica alcuni strumenti per perseguire l'obiettivo di garantire libertà e diritti degli interessati; uno di questi è la "Valutazione d'impatto sulla protezione dei dati" (art. 35), da effettuare quando un nuovo tipo di trattamento può comportare un rischio elevato per la libertà e i diritti degli interessati; ad esempio, quando si trattano su larga scala dati riguardanti condanne penali e reati, oppure riguardanti le opinioni politiche, la religione, la salute o le relazioni sessuali ed altre tipologie di dati personali meritevoli di particolare protezione⁶. Gli archivisti potranno avere la necessità di effettuare una valutazione d'impatto quando devono progettare la creazione di uno strumento di ricerca relativo all'archivio di un carcere o di un partito politico; se oggi si volesse creare un portale come "Carte da legare" (<http://www.cartedalegare.san.beniculturali.it>), relativo agli archivi degli ospedali psichiatrici, si dovrebbe senz'altro effettuare preventivamente una valutazione d'impatto. Ma non bisogna confondere il fine con il mezzo: il punto non è produrre un ennesimo pezzo di carta da poter esibire in caso di controlli, ma programmare in modo accurato i trattamenti di dati personali particolarmente delicati, in modo da prevenire il rischio di danneggiare seriamente delle persone.

Gli archivisti in genere hanno già l'abitudine a valutare con attenzione i possibili rischi per gli interessati, prima di pubblicare on line o diffondere in altro modo documenti o strumenti di ricerca contenenti dati personali, così come hanno già l'abitudine ad ottemperare ad altri obblighi previsti dal GDPR; utilizzano però una diversa terminologia. Questo è fonte di incomprensioni e di timori fuori posto.

Secondo il GDPR (così come secondo la direttiva del 1995), uno dei principi fondamentali applicabili al trattamento dei dati personali è la minimizzazione dei dati (art. 5,

c. 1, lett. c). Questo principio non conosce eccezioni: deve essere applicato anche in caso di trattamenti finalizzati all'archiviazione nel pubblico interesse. A prima vista, sembra minaccioso per gli archivi, ma in realtà gli archivisti lo hanno sempre applicato, solo che lo chiamano in modo diverso, cioè "scarto". Quando selezionano per la conservazione permanente solo una percentuale limitata dei documenti prodotti da un ente nel corso della sua attività e scartano il resto, gli archivisti stanno minimizzando i dati personali che verranno archiviati. Quindi stanno contemporaneamente mettendo in pratica uno dei cardini della professione archivistica e uno dei principi del GDPR. Il regolamento europeo ci richiede di essere in grado di spiegare i motivi della nostra selezione; anche in questo caso, buona pratica archivistica e protezione dei dati personali vanno mano nella mano. Se non siamo in grado di spiegare perché abbiamo scelto di conservare una serie documentaria e scartarne un'altra vuol dire che siamo professionalmente inadeguati.

Un simile rafforzamento reciproco di protezione dei dati personali e buona pratica archivistica si riscontra anche in materia di sicurezza dei dati. Il GDPR include tra i principi applicabili al trattamento dei dati personali quello della «integrità e riservatezza», ai sensi del quale i dati debbono 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 (art. 5, c. 1, lett. f)

Questo principio viene articolato in prescrizioni nell'art. 32 dedicato alla "Sicurezza del trattamento". Per "sicurezza" non si intende solo la "riservatezza" dei dati; il titolare deve anche essere in grado di assicurare "l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;" (art. 32, c. 1, lett. b) e c). La perdita o distruzione di documenti contenenti dati personali che dovrebbero essere conservati si configura dunque come una violazione del GDPR (oltre che, nel caso delle PA, come una violazione delle norme sul documento amministrativo e del Codice dei beni culturali). Il timore delle severe sanzioni previste dal GDPR potrà quindi giocare a favore di una maggiore attenzione per la conservazione degli archivi.

Dal punto di vista archivistico, la più vistosa novità introdotta dal GDPR rispetto alla direttiva 95/46/CE è costituita dal fatto che mentre precedentemente non vi erano specifiche deroghe a favore degli archivi (la direttiva prevedeva solo deroghe a favore della ricerca storica), il GDPR distingue tra le deroghe a favore dell'«archiviazione nel pubblico interesse» e quelle a favore della ricerca storica. Questa distinzione ha recato dei vantaggi (la necessità della conservazione degli archivi è affermata esplicitamente) e degli svantaggi, costituiti dalla contorta e limitativa definizione di cosa costituisca «archiviazione nel pubblico interesse», contenuta in una delle considerazioni preliminari (il "considerando" 158), che tra l'altro è stata anche tradotta male in italiano⁷.

Non è questa la sede per addentrarsi in una discussione della definizione di «archiviazione nel pubblico interesse» e degli altri punti critici o di difficile interpretazione del GDPR. Per una sintetica trattazione di questi temi si rinvia alle *Linee guida del*

Gruppo Europeo degli Archivi per l'applicazione nel settore archivistico del Regolamento europeo sulla protezione dei dati personali, scaricabili gratuitamente dal sito della Direzione generale archivi, dove si possono trovare anche i link alle videoregistrazioni di due convegni dedicati all'applicazione del GDPR negli archivi, organizzati dalla DGA, "La conservazione archivistica nell'era del GDPR" (Roma, 30 gennaio 2019) e "Il GDPR in archivio: strumenti di lavoro per l'applicazione del Regolamento europeo protezione dati personali" (Roma, 13 marzo 2019)⁸.

In questa sede sarà sufficiente ricordare che la chiave di volta per superare i principali pericoli per gli archivi creati dall'applicazione del GDPR è costituita dalla creazione dei piani di conservazione: sono questi, infatti, lo strumento che permette di affermare che una determinata serie documentaria è destinata alla "archiviazione nel pubblico interesse" e dunque può essere legittimamente conservata nella sua integrità. Purtroppo, molti enti pubblici e privati ne sono privi; produrli sarà la grande sfida che gli archivisti dovranno affrontare nel prossimo futuro, se vogliono evitare che l'applicazione del GDPR si traduca in indiscriminate distruzioni dei documenti contenenti dati personali.

In breve, il GDPR pone effettivamente alcuni problemi applicativi negli archivi, ma le demonizzazioni che circolano sono senz'altro fuori luogo. Le buone pratiche archivistiche possono infatti rendere pienamente compatibile il GDPR con la conservazione documentaria.

¹ *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).*

² Si vedano ad esempio: *Cosa sono i big data e perché sono così importanti* (che cita un articolo dell'«Economist»), 25 dicembre 2017, in SkyTG24, <<https://tg24.sky.it/tecnologia/2017/12/19/big-data-cosa-sono.html>>, e Andrea Daniele Signorelli, *I dati sono il nuovo petrolio: e se li nazionalizzassimo?*, in Wired", 7 aprile 2018, <<https://www.wired.it/attualita/tech/2018/04/07/nazionalizziamo-big-data/>>.

³ *L'universo dei dati e la libertà della persona*. Discorso del Presidente Antonello Soro (Roma, 7 maggio 2019), p. 5, <<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9109075>>.

⁴ In Italia, la legge 31 dicembre 1996, n. 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, successivamente modificata e infine confluita nel d.lgs. 30 giugno 2003, n.196 *Codice in materia di protezione dei dati personali*.

⁵ Le *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*, sono state pubblicate sulla Gazzetta Ufficiale n. 12 del 15 gennaio 2019.

⁶ La precedente normativa li definiva "dati sensibili"; questa espressione non compare più nel GDPR, sostituita da "categorie particolari di dati personali di cui all'articolo 9". Il GDPR non usa più neppure l'espressione "dati giudiziari", sostituita da "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza" (art.10).

vedi anche

Notiziario della Sezione Ligure dell'Associazione Italiana Biblioteche

Vol. 29 N° 1 (2019) - ISSN 2281-0617

[7](#) Mi permetto al riguardo di rinviare al mio *Lost in translation: errori di traduzione nel Regolamento europeo protezione dati personali*, in "Il Mondo degli archivi" 29 ottobre 2018.

[8](http://www.archivi.beniculturali.it/index.php/strumenti) <http://www.archivi.beniculturali.it/index.php/strumenti>