IL TRATTAMENTO A FINI DI RICERCA DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI. A PROPOSITO DEL GDPR[1]

Giulia Barrera

Title: GDPR and the processing of personal data relating to criminal convictions and offences for research purposes

Abstract

Under the General Data Protection Regulation (UE) 2016/679, the processing of personal data relating to criminal convictions and offences is lawful only if authorised by Member State law. In Italy, a ministerial decree will dictate which kinds of processing are allowed, apart from those already authorised by the law. This article argues that such a decree should authorise the processing of court-case files' copies for the purpose of documentation, study and research.

Keywords: General Data Protection Regulation, GDPR, personal data relating to criminal convictions and offences, freedom of expression

Ai sensi del Regolamento (UE) 2016/679 relativo alla protezione dei dati personali (GDPR), il trattamento dei dati personali inerenti a condanne penali e reati è lecito solo se previsto dal diritto degli stati membri. L'articolo richiama l'attenzione sulla necessità che il decreto ministeriale che dovrà indicare i trattamenti leciti – oltre a quelli già previsti dalla legge – includa i trattamenti a fini di documentazione, studio e ricerca, delle riproduzioni dei fascicoli processuali.

Parole chiave: Regolamento (UE) 2016/679, Protezione dati personali, "dati personali relativi a condanne penali e reati", libertà di espressione

[1] Versione riveduta e ampliata della relazione "Dati penali negli archivi: cosa cambia con il GDPR?" presentata alla giornata di studi: "La conservazione archivistica nell'era del GDPR: il nodo degli archivi privati e dei dati penali" (Roma, Ministero per i beni e le attività culturali, 30 gennaio 2019), organizzata dalla Direzione generale archivi, dall'Istituto centrale per gli archivi (ICAR) e dall'Associazione nazionale archivistica italiana (ANAI). La registrazione dell'incontro è disponibile sul sito dell'ICAR, alla url: http://www.icar.beniculturali.it/index.php?id=374.

1. Introduzione

Il regolamento europeo in materia di protezione dei dati personali (noto con l'acronimo inglese GDPR)[2] permette il trattamento dei "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza" solo se previsto dal diritto degli Stati membri. In Italia, il ministro della giustizia dovrà emanare un decreto che individui quali trattamenti di tali tipologie di dati siano consentiti, oltre a quelli già autorizzati da legge o regolamento[3]. Queste pagine hanno il fine di richiamare l'attenzione sull'opportunità che il decreto autorizzi, fra gli altri, i trattamenti a fini di documentazione, studio e ricerca, non solo delle riproduzioni delle sentenze (come è avvenuto fino ad oggi), ma anche delle riproduzioni dei fascicoli processuali.

In Italia, operano decine di associazioni di familiari di vittime di stragi terroristiche o di mafia, nonché centri di documentazione sulla mafia e sul terrorismo (come ad esempio l'Associazione parenti delle vittime della strage di Ustica, l'Associazione tra i familiari delle vittime della strage della stazione di Bologna del 2 agosto 1980, la Casa della memoria di Brescia o il Centro siciliano di documentazione "Giuseppe Impastato") che conservano copie di fascicoli processuali, al fine di offrire supporto alle battaglie perché sia resa giustizia alle vittime, mantenere viva la memoria sui più gravi episodi di criminalità mafiosa e di terrorismo che hanno insanguinato l'Italia e promuovere studi e ricerche al riguardo.

Per iniziativa del Centro di documentazione Archivio "Flamigni", nel 2005 decine di queste associazioni di familiari di vittime e centri studi hanno costituito la "Rete degli archivi per non dimenticare"[4]. La Rete ha stretto rapporti di collaborazione con uffici giudiziari e con Archivi di Stato, per progetti di digitalizzazione dei fascicoli

[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).*

[3] Art. 2-octies del 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.*

[4] *Rete degli archivi per non dimenticare. Guida alle fonti per una storia ancora da scrivere*, a cura di Ilaria Moroni, Roma: Istituto centrale per il restauro e la conservazione del patrimonio archivistico e librario, 2010.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

processuali[5]. Dal 2011, grazie alla Direzione generale archivi e all'Istituto centrale per gli archivi, la Rete fruisce di un portale ad hoc nell'ambito del Sistema archivistico nazionale[6], cui è affiancato un archivio virtuale che permette di consultare le riproduzioni digitali di atti processuali (relativi alla strage di Brescia del 28 maggio 1974, all'omicidio di Ilaria Alpi e Miran Hrovatin, alla strage di Piazza Fontana, ecc.) e di commissioni parlamentari d'inchiesta (come quelle sulla loggia P2 o sul caso Moro)[7].

Dal punto di vista della normativa sulla protezione dei dati personali, non rileva se i dati siano contenuti in documenti originali o in copie: ciò che conta è la qualità dei dati, ed indiscutibilmente quando un'associazione di familiari conserva la copia di un fascicolo processuale, lo indicizza e ne promuove la consultazione, sta trattando "dati personali relativi a condanne penali e a reati".

Oltre alle associazioni dei familiari, alle fondazioni e ai centri di documentazione riuniti nella Rete degli archivi per non dimenticare, possono trattare "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza" per finalità di documentazione, studio o ricerca anche altri soggetti della società civile, come ad esempio centri studi di taglio accademico, associazioni che si occupano dei diritti dei detenuti o più in generale della difesa dei diritti umani.

La scelta del legislatore europeo e nazionale di porre severe limitazioni al trattamento dei "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza" è del tutto condivisibile. Sarebbe paradossale, però, se tali limiti finissero per porre ostacoli ad enti che hanno lo scopo di promuovere la conoscenza di fenomeni criminali, al fine di contrastarli. Il GDPR affida al diritto degli Stati membri il ruolo di conciliare la protezione dei dati personali con la libertà di espressione e di informazione. Occorre dunque che l'Italia si avvalga di questa facoltà.

---

[5] Ilaria Moroni, *Terrorismi e mafie: una storia ancora da scrivere #9maggio*, in "Il Mondo degli archivi", 8 maggio 2017, www.ilmondodegliarchivi.org/component/content/article?id=498:terrorismi-e-mafie-una-storia-ancora-da-scrivere-9maggio.

[6] www.memoria.san.beniculturali.it Il Sistema archivistico nazionale – SAN è il punto di accesso unificato alle risorse archivistiche nazionali rese disponibili sul web da sistemi informativi, banche dati e strumenti di ricerca digitali sviluppati a livello nazionale, regionale e locale dallo Stato, dalle Regioni e da altri soggetti pubblici e privati.

[7] www.fontitaliarepubblicana.it/DocTrace/.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

Il problema che si solleva in queste pagine è di carattere giuridico, tuttavia non viene affrontato con l'occhio del giurista, ma dell'archivista. Per la natura della loro professione e per precisi obblighi deontologici che gli derivano da codici di condotta nazionali e internazionali[8], gli archivisti, che nelle sale di studio degli Archivi debbono mettere in pratica quotidianamente le norme sulla consultabilità dei documenti[9], si confrontano costantemente con i dilemmi del bilanciamento tra diritto di accesso ai documenti e diritto alla protezione dati personali, interesse pubblico alla conoscenza e tutela della dignità della persona. Al dibattito sul trattamento dei dati personali gli archivisti possono contribuire con questo bagaglio di esperienze.

Nella prima parte di questo articolo, vengono ricordati alcuni esempi di uso a fini di lucro dei dati personali sulle condanne penali, effettuati oltreoceano, al fine di ricordare al lettore quanto sia opportuno che la normativa europea a protezione dei dati personali includa severi limiti al trattamento di questa tipologia di dati. Nella seconda parte, si descrive l'attuale quadro normativo in materia (ricordando anche brevemente quale fosse la normativa prima dell'approvazione del regolamento europeo), ed infine viene illustrata in modo più articolato la proposta – già menzionata – di autorizzare i trattamenti a fini di documentazione, studio e ricerca, non solo delle riproduzioni delle sentenze, ma anche delle riproduzioni dei fascicoli processuali, con adeguate garanzie per le libertà e i diritti degli interessati.

[8] Il Consiglio internazionale degli archivi (l'organizzazione mondiale delle istituzioni archivistiche, delle associazioni di archivisti e dei singoli archivisti, con soci da 199 paesi e territori) si è dotata nel 1996 di un *Codice internazionale di deontologia degli archivisti*; nel 2012 ha approvato i *Principi sull'accesso agli archivi*. In Italia, nel 2001 il Garante protezione dati personali approvò il *Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici*, poi divenuto all. 2 del Codice protezione dati personali, ed oggi ribattezzato *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* - 19 dicembre 2018.

[9] D.Lgs. 22 gennaio 2004, n. 42 *Codice dei beni culturali e del paesaggio*, artt. 122-127.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

2. Il business dei dati penali: esempi da oltreoceano

Il 30 gennaio del 2017, il Tribunale federale di Ottawa, in Canada, emise una sentenza contro il cittadino rumeno Sebastian Radulescu, proprietario di Globe24h.com, un sito che affermava di diffondere informazioni pubbliche, soprattutto governative, per finalità giornalistiche[10]. Il sito Globe24h.com era stato denunciato da un cittadino canadese (A.T.), dopo aver scoperto che cercando il suo nome su Google emergeva una sentenza penale che lo riguardava, posta on line dal sito Globe24h.com. Non si trattava di un caso isolato: già decine di altre persone avevano denunciato fatti analoghi all'autorità garante per la protezione dati personali canadese (Office of the Privacy Commissioner of Canada, OPCC).

In Canada vengono pubblicate on line molte più sentenze che in Italia. Il Canadian Law Information Institute (CanLII, una organizzazione senza scopo di lucro creata dalla Federazione degli ordini degli avvocati canadesi) pubblica sul proprio sito le sentenze delle corti federali e statali di ogni ordine e grado, per un totale che attualmente supera i 2 milioni e trecentomila sentenze[11]. Il sito del CanLII non permette l'indicizzazione delle sentenze da parte dei motori di ricerca generalisti: per trovare una sentenza, occorre entrare nel sito[12].

Il sito rumeno Globe24h.com, invece, dopo aver scaricato in massa le sentenze dal sito del Canadian Law Information Institute, nel 2013 aveva iniziato a ripubblicarle sul proprio sito, rendendole ricercabili da Google e da altri motori di ricerca, così che cercando un nome di persona su Google, poteva capitare di avere tra i risultati una sentenza canadese. Avevano in tal modo iniziato a circolare sul web questioni molto personali, come divorzi o altre controversie familiari, nonché informazioni sulle condizioni di salute delle persone o altri dati sensibili e sensibilissimi contenuti nelle

[10] A.T. c. Globe24h.com, 2017 CF 114 (CanLII), <http://www.canlii.ca/t/h31qn>. Per una breve sintesi del caso si veda: Pierre–Luc Déziel, *Le droit à l'oubli au Canada: l'affaire Globe24h et le rôle du juge dans les requêtes de déréférencement*, in *The Right to be Forgotten in Europe and Beyond / Le droit à l'oubli en Europe et au-delà*, Olivia Tambou, Sam Bourton (Eds.), Blogdroiteuropéen, Luxembourg, 2018, pp. 106-8. Available at: https://wp.me/p6OBGR-2QK.

[11] Il CanLII ospita più di 300 basi di dati, relative alle sentenze e decisioni di tribunali civili e militari, autorità indipendenti, collegi degli ordini professionali, ecc. www.canlii.org/en/databases.html.

[12] Unica eccezione è costituita dalle sentenze della Corte suprema del Canada, di cui il CanLII permette l'indicizzazione da parte di motori di ricerca esterni. Sulla linea in materia di privacy dell'Istituto si veda www.canlii.org/en/info/privacy.html.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

sentenze; ben presto, quindi, diversi cittadini canadesi si rivolsero alla loro autorità garante, denunciando le attività del sito Globe24h.com.

Queste persone in genere sapevano che le sentenze in Canada sono pubbliche e pubblicate, e non si dolevano di ciò. Ciò che motivava il loro ricorso era il fatto che una ricerca casuale del loro nome su Google – effettuata magari da un compagno di scuola dei figli o da un vicino di casa – facesse emergere la sentenza che li riguardava. Si erano dunque rivolti al sito Globe24h.com chiedendo la rimozione delle sentenze che li riguardavano, sentendosi in risposta proporre due opzioni: pagare per ottenere una rapida rimozione; oppure compilare un modulo fornendo le proprie generalità, allegare la copia di un documento di identità (formalità non richieste per la rimozione a pagamento) ed attendere fino a sei mesi per la procedura gratuita di rimozione. Oltre a ciò, alcuni cittadini, dopo aver pagato, si erano resi conto che altre versioni della sentenza erano rimaste on line.

Nonostante il sito Globe24h.com sostenesse di avere finalità giornalistiche e dunque di essere protetto dalle norme a garanzia della libertà di informazione; e ricordasse che comunque pubblicava sul suo sito sentenze che erano pubbliche e già on line sul sito del Canadian Law Information Institute, il Tribunale federale canadese condannò Sebastian Radulescu per violazione della legge canadese sulla protezione dati personali[13] e gli ordinò di rimuovere dal sito Globe24h.com tutte le sentenze canadesi, nonché di intraprendere i passi necessari per la rimozione delle sentenze dalla memoria *caches* dei motori di ricerca. Una decisione pienamente condivisibile. Il sito Globe24h.com faceva un uso dei dati penali per finalità di lucro che rasentavano l'estorsione, ed oggi non esiste più. Sono invece attivi negli Stati Uniti siti che raccolgono sistematicamente dati giudiziari su singole persone, attingendo alle banche dati pubbliche e li vendono alla propria clientela.

Negli Stati Uniti non vi è una legge federale analoga al GDPR, che protegga in modo complessivo i dati personali. Esistono diverse leggi federali relative a specifiche tipologie di dati o a specifici ambiti, come il Fair Credit Reporting Act, che dispone che le agenzie che producono rapporti sulla affidabilità delle persone dal punto di vista creditizio (*consumer reporting agency*), non possono includere informazioni

[13] Personal Information Protection and Electronic Documents Act, SC 2000, c 5 (noto con l'acronimo PIPEDA).

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

risalenti oltre un certo numero di anni (10 anni per la bancarotta, in genere 7 anni per gli arresti, ecc.)[14]. Anche i singoli Stati hanno legiferato in materia, garantendo gradi di protezione molto diversificati[15]. Il quadro complessivo è di una tutela inferiore a quella di cui godiamo in Europa, come dimostra proprio il caso del trattamento dei dati relativi alle condanne penali e ai reati.

È potuta infatti emergere "un'industria privata che ripesca, vende e spesso sensazionalizza le fedine penali. Questa industria ha reso l'accesso alle informazioni sulla storia delle condanne penali di un individuo facile, economica, onnipresente e illimitata nel tempo."[16]

Anche le foto dei detenuti effettuate nelle stazioni di polizia (mugshot) corredate dalle generalità del detenuto ed altre informazioni personali (compresa l'accusa che ha determinato l'arresto) sono diffuse negli Stati Uniti da un fiorire di siti commerciali. Come spiega Andrea Slane, il "modello di business" di questo genere di siti prevede che gli interessati possano – pagando – far rimuovere i dati che li riguardano. Qualche Stato proibisce queste pratiche, come la California, che nel maggio 2018 ha accusato il sito Mugshots.com di estorsione e altri reati, ma per la maggior parte degli Stati si tratta di una attività legittima.

In Italia, invece, non solo la legge – come si vedrà in dettaglio più avanti – non permette un simile uso commerciale di dati personali penali, ma anche nel caso di un loro legittimo trattamento nell'ambito di attività giornalistica, pone severi limiti all'utilizzo di foto di detenuti. Le regole deontologiche per i giornalisti, infatti, stabiliscono che "Salvo rilevanti motivi di interesse pubblico o comprovati fini di giustizia e di polizia, il giornalista non riprende né produce immagini e foto di persone in stato di detenzione senza il consenso dell´interessato". (art. 8, c. 2).

[14] Andrea Slane, *Information Brokers, Fairness, and Privacy in Publicly Accessible Information*, in "Canadian Journal of Comparative and Contemporary Law", 2018, vol. 4, n. 1, pp. 249-291.

[15] Per una panoramica sintetica, si veda Luis Acosta, *The right to respect for private life: digital challenges, a comparative-law perspective: The United States*, European Parliamentary Research Service, Brussels, 2018.

[16] Alessandro Corda, *More Justice and Less Harm: Reinventing Access to Criminal History Records* in "Howard Law Journal", 2016, vol. 60, n. 1, p. 3.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

Inoltre, "Le persone non possono essere presentate con ferri o manette ai polsi, salvo che ciò sia necessario per segnalare abusi." (art. 8 c. 3)[17].

Negli USA, più ancora che dalle tariffe sulla rimozione, osserva ancora Slane, siti che pubblicano le foto delle persone arrestate guadagnano dagli introiti pubblicitari, relativi soprattutto a due tipi di servizi on line: da un lato, servizi di rimozione o oscuramento di foto e notizie dell'arresto ed altre notizie negative, dai risultati di Google e Bing, per ricerche effettuate utilizzando un determinato nome come chiave di ricerca[18]; da un altro, vengono pubblicizzati siti che, a pagamento, forniscono un profilo biografico di persone comuni, compilato collazionando una varietà di dati attinti da fonti pubbliche e private, primo fra tutti gli equivalenti locali del nostro casellario giudiziale (BeenVerified.com, Peoplelooker.com, Instantcheckmate.com, ecc.)[19]. Ad esempio Truthfinder.com promette ai potenziali clienti di soddisfare le loro curiosità su amici, parenti e conoscenti; a pagamento, il sito – che si vanta di scandagliare anche il deep web e di recuperare persino pagine web cancellate – è pronto a fornire data di nascita, indirizzo, elenco delle proprietà immobiliari, stato di famiglia, multe, fedina penale, storia scolastica e lavorativa, nonché notizie su amici, partner sentimentali attuali e passati, e così via. Fra questi dati, quelli penali sono particolarmente apprezzati dai clienti dei siti tipo Truthfinder.com.

Come ha osservato Alessandro Corda, oggi negli Stati Uniti i controlli sulle fedine penali altrui sono diventati prassi comune. Le fedine penali sono "regolarmente passate al vaglio da potenziali datori di lavoro, padroni di casa e università, e spesso da vicini di casa, conoscenti e partner"[20]. Prima dell'assunzione, il 90% dei datori di lavoro controlla la fedina penale dei candidati.[21] In Italia, invece, i datori di lavoro possono accedere alla fedina penale dei lavoratori solo in casi specifici indicati dalla legge o da un provvedimento del Garante. Nell'ultima autorizzazione generale emanata, il Garante ha autorizzato i datori di lavoro al trattamento dei dati giudiziari, solo qualora sia "*indispensabile* per […] adempiere o esigere

[17] *Regole deontologiche relative al trattamento di dati personali nell'esercizio dell'attività giornalistica pubblicate ai sensi dell'art. 20, comma 4, del D.lgs. 10 agosto 2018, n. 101,* 29 novembre 2018 (Pubblicate sulla Gazzetta Ufficiale n. 3 del 4 gennaio 2019).
[18] Si veda ad esempio www.removearrest.com/
[19] Andrea Slane, *op. cit*.
[20] Alessandro Corda, *More Justice*, *op. cit*., p. 3
[21] Alessandro Corda, *More Justice*, *op. cit.*, p. 19.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

l'adempimento di specifici obblighi o eseguire specifici compiti previsti da leggi, dalla normativa dell'Unione europea, da regolamenti o da contratti collettivi, anche aziendali, e ai soli fini della gestione del rapporto di lavoro"[22] (corsivo aggiunto). Può dare un'idea della distanza che ci separa dalle prassi di oltreoceano un caso su cui ha deliberato il Garante a maggio 2018 relativo ad una società cooperativa che gestiva magazzini di prodotti finiti (vestiario, cosmetici, ecc.), che aveva chiesto l'autorizzazione ad acquisire il certificato del casellario giudiziale dei dipendenti, perché all'interno dei depositi presso cui operava si verificavano frequenti furti. Il Garante ha negato l'autorizzazione, in quanto il trattamento sarebbe stato privo di una base giuridica, anche in considerazione del fatto che le condizioni di ammissione alla cooperativa non includevano lo "specifico requisito di onorabilità".[23]

Negli Stati Uniti, l'indiscriminata diffusione dei dati relativi alle condanne penali costituisce un forte ostacolo al reinserimento sociale delle persone che hanno commesso reati, con un conseguente danno per loro stessi e per la società nel suo complesso[24]. "Per un individuo – spiega ancora Corda – diventa pressoché impossibile lasciarsi alle spalle il proprio passato criminale."[25]

Ben vengano, dunque, le limitazioni al trattamento dei "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza" poste dal GDPR.

[22] Garante per la protezione dei dati personali, Autorizzazione n. 7/2016, *Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici* (efficace dal 1° gennaio 2017 fino al 24 maggio 2018, data di entrata in vigore del GDPR).

[23] Garante per la protezione dei dati personali, Provvedimento del 22 maggio 2018, n. 317. Sulla stessa linea anche altri provvedimenti del Garante sul trattamento dei dati giudiziari dei dipendenti, come il n. 267 del 15 giugno 2017.

[24] Alessandro Corda, *More Justice*, *op. cit.*, passim ?.

[25] Alessandro Corda, *Beyond Totem and Taboo: Toward a Narrowing of American Criminal Record Exceptionalism*, in "Federal Sentencing Reporter", 2018, vol. 30, nn. 4-5, p. 241.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

3. La normativa sul trattamento a fini di documentazione e ricerca dei dati personali relativi a condanne penali e reati

Nell'Unione Europea, il GDPR protegge i cittadini da usi delle fedine penali che possono comportare rischi per i diritti e le libertà degli interessati, con l'articolo 10 (*Trattamento dei dati personali relativi a condanne penali e reati*), che recita:

> "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, 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. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

Le restrizioni poste dall'art. 10 non prevedono eccezioni (se non quelle previste dall'art. 85, relativo ai trattamenti a scopi giornalistici o di espressione accademica, artistica o letteraria, di cui si dirà più avanti). Si noti, a questo punto, la differenza rispetto alle restrizioni al trattamento delle "categorie particolari di dati personali" (che precedentemente il Codice protezione dati personali chiamava "dati sensibili"). L'art. 9 del GDPR vieta di trattare i dati personali che

> "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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". (c. 1)

Ma introduce ben dieci eccezioni a tale divieto, una delle quali si applica quando il trattamento è necessario "a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" (art. 9, c. 2, lett. j). Questa espressione ricorre ripetutamente nel GDPR, perché sono previste numerose eccezioni e deroghe nel caso di trattamenti per tali finalità; in alcuni casi, è lo stesso GDPR a disciplinare le deroghe[26], in altri, viene invece data facoltà agli Stati membri di introdurle[27]. Nel

[26] L'art. 5 prevede eccezioni ai principi della "limitazione della finalità" e della "limitazione della conservazione" nel caso i dati siano trattati a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. Deroghe per queste tipologie di trattamenti sono previste anche dagli articoli 9 (*Trattamento di categorie particolari di dati personali*), 14 (*Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato*) e 17 (*Diritto alla cancellazione ("diritto all'oblio"*).

[27] L'art. 89 accorda al diritto dell'Unione o degli Stati membri la facoltà di prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21 nel caso di trattamenti di dati personali "per finalità di archiviazione nel pubblico interesse" (c. 3) e ai diritti di cui agli articoli 15, 16, 18 e 21 nel caso di trattamenti "a fini di ricerca scientifica o storica o a fini statistici" (c. 2).

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

caso del trattamento dei dati relativi alle condanne penali, invece, non vi è una previsione di deroga per trattamenti a fini archivistici o di ricerca.

Per inciso, occorre osservare che non è affatto chiaro quali archivi privati rientrino nella definizione di "archiviazione nel pubblico interesse"; comunque, come si è visto, anche se un centro studi privato venisse riconosciuto come ente che effettua "archiviazione nel pubblico interesse", questo non lo legittimerebbe a trattare dati personali relativi a condanne penali.

I limiti posti dall'art. 10 non ostacolano la conservazione degli atti dei tribunali da parte degli Archivi di Stato; in questo caso, infatti, concorrono tutte e due le circostanze che rendono lecito il trattamento dei dati penali: a) avviene sotto il controllo dell'autorità pubblica; b) è autorizzato da una legge che prevede garanzie per i diritti e le libertà degli interessati[28].

Diverso è invece il caso del trattamento di copie di fascicoli processuali da parte di privati, a fini di documentazione, studio e ricerca. Per capire bene i termini del problema, è opportuno fare un passo indietro e vedere come era fino ad oggi regolata la materia.

La direttiva europea del 1995 sul trattamento dei dati personali dedicava ai dati penali il comma 5 dell'articolo 8 (*Trattamenti riguardanti a categorie particolari di dati*), che poneva restrizioni tutto sommato simili a quelle imposte dal GDPR.

> "5. I trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza possono essere effettuati solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che possono essere fissate dallo Stato membro in base ad una disposizione nazionale che preveda garanzie appropriate e specifiche. Tuttavia un registro completo delle condanne penali può essere tenuto solo sotto il controllo dell'autorità pubblica."[29]

[28] Il Codice dei beni culturali e del paesaggio (D.lgs. 42/2004) prevede infatti il versamento degli atti degli organi giudiziari agli Archivi di Stato (art. 41) e ne limita la consultabilità (art. 122).

[29] *Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

In Italia, la legge 675/1996 che recepì la direttiva europea, ammetteva il trattamento dei dati che compaiono nel casellario giudiziario "soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante" [30].

Sette anni dopo, il Codice in materia di protezione dei dati personali (D.lgs 196/2003) – che coordinò le norme che si erano affastellate nel frattempo – presentava una definizione più articolata del tipo di dati protetti e delle misure a loro protezione; non parlava di dati relativi a condanne penali, bensì di "dati giudiziari". Cosa si intendesse con questa espressione era definito dall'art. 4, c. 1, lett. e); si trattava in sostanza dei dati del casellario giudiziale e dell'anagrafe delle sanzioni amministrative, dei carichi pendenti e della qualità di imputato o indagato. Oggi, a seguito dell'emanazione del D.lgs. 101/2018[31], che ha adeguato la normativa italiana al regolamento europeo protezione dati personali, questa definizione è stata abrogata, così come sono stati abrogati gli articoli 21, 22 e 27 del Codice protezione dati personali, relativi al trattamento dei dati giudiziari, perché la materia è già disciplinata dal GDPR. Ma il GDPR non reca una definizione di "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza". Dunque una prima differenza della regolamentazione attuale rispetto alla normativa previgente consiste nel fatto che l'oggetto della limitazione al trattamento non sono più i "dati giudiziari", definiti in modo circostanziato, bensì i "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza", una espressione che sembra considerevolmente più estensiva e di cui è auspicabile vengano chiariti i confini.

Questo fatto, per inciso, ha ricadute anche sulla consultabilità dei documenti d'archivio, compresi i fascicoli processuali conservati dagli Archivi di Stato, poiché il Codice dei beni culturali esclude dalla consultazione per 40 anni "i dati relativi a provvedimenti di natura penale espressamente indicati dalla normativa in materia

[30] L. 31 dicembre 1996, n. 675 *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, Art. 24 (*Dati relativi ai provvedimenti di cui all'articolo 686 del codice di procedura penale*). L'art. 686 (*Iscrizione nel casellario giudiziale*) del Cpp – poi abrogato – elencava quali dati dovessero essere iscritti nel casellario giudiziario.

[31] D.Lgs. 10 agosto 2018, n. 101 *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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).*

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

di trattamento dei dati personali"[32]. Quindi oggi dobbiamo considerare esclusi dalla consultazione per 40 anni i "dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza." Bisogna inoltre ricordare a questo proposito che invece, ai sensi dell'art. 116 del Codice di procedura penale, i fascicoli processuali, quando sono ancora conservati negli archivi degli uffici giudiziari, possono essere consultati da "chiunque vi abbia interesse", su autorizzazione del magistrato competente. Questo disallineamento è stato già più volte segnalato dagli archivisti, che sollecitano anche per gli atti processuali versati negli Archivi di Stato una disciplina più liberale[33].

Altra innovazione è costituita dal cambiamento dell'autorità che dovrà indicare i trattamenti consentiti, oltre a quelli autorizzati dalla legge. Il D.lgs 196/2003 consentiva il trattamento dei dati giudiziari solo se autorizzato "da espressa disposizione di legge o provvedimento del Garante". Ora, invece, a seguito delle modifiche del Codice introdotte dal D. lgs. 101/2018, sarà il ministro della giustizia che – sentito il Garante – potrà per decreto autorizzare ulteriori trattamenti (D lgs. 196/2003, art. 2-octies, c. 2).

Il Garante fino al 2016 ha emanato periodicamente delle autorizzazioni di carattere generale, in cui indicava quali soggetti potessero trattare dati penali, a quali fini e in che termini. Ad esempio, venivano autorizzati gli avvocati a trattare i dati dei loro clienti, o le compagnie di assicurazione a trattare quelli relativi ai sinistri, secondo parametri ben definiti. Un capo di questo provvedimento di autorizzazione generale era dedicato alla "Documentazione giuridica". L'autorizzazione emanata dal Garante nel 2016 così recitava:

> "L´autorizzazione è rilasciata per il trattamento, ivi compresa la diffusione, di dati relativi a sentenze e altri provvedimenti giurisdizionali, per finalità di informazione giuridica, ovvero di documentazione, di studio e di ricerca in campo giuridico. Il trattamento, disciplinato dagli artt. 51 e 52 del Codice, deve essere effettuato nel rispetto delle indicazioni fornite nelle "Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di

[32] Art. 122, c. 1, lett. b), del D. lgs. 42/2004. Il successivo art. 123 però prevede la possibilità di ottenere, "per scopi storici", l'autorizzazione alla consultazione dei documenti prima che siano maturati i termini di esclusione.

[33] Si veda da ultimo Stefano Twardzik, *La consultabilità dei documenti*, in *Archivistica. Teorie, metodi, pratiche*, Linda Giuva e Maria Guercio (a cura di), Carocci, Roma, 2014, pp. 237-261.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

> informazione giuridica." (deliberazione del Garante del 2 dicembre 2010, G.U. 4 gennaio 2011, n. 2)"[34].

Venivano dunque autorizzati i trattamenti per finalità di "documentazione, studio e ricerca", una definizione che ben si attaglia alle tipologie di trattamenti effettuati dalla Rete degli archivi per non dimenticare e da altri centri di ricerca. Però si circoscriveva l'autorizzazione al trattamento dei "dati relativi a sentenze e altri provvedimenti giurisdizionali", mentre in molti casi i centri di ricerca o le associazioni di familiari – come si è già segnalato – trattano anche copie dei fascicoli processuali. Sarebbe opportuno che il decreto di autorizzazione del ministro della giustizia superasse questo limite.

4. Garanzie per la dignità, i diritti e le libertà fondamentali della persona

Diffondere on line il contenuto di sentenze può, in certi casi, ledere la dignità e i diritti degli interessati. Per questo, l'art. 52 del Codice protezione dati personali tuttora in vigore dispone alcune misure a tutela degli interessati, che è utile ricordare brevemente prima di considerare quali garanzie siano appropriate in caso di trattamento di fascicoli processuali.

Salvo specifiche eccezioni, afferma l'art. 52, "è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali". Le eccezioni – il cui contenuto è spiegato in modo più articolato nelle *Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica* pubblicate dal Garante – in sintesi sono le seguenti:

1) È sempre obbligatorio omettere, nelle riproduzioni delle sentenze, qualsiasi dato che permetta di identificare minori coinvolti nei provvedimenti giudiziari. Non è sufficiente omettere i nomi dei minori: occorre omettere anche informazioni quali i

[34] Garante per la protezione dei dati personali, Autorizzazione n. 7/2016, *Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici* (efficace dal 1° gennaio 2017 fino al 24 maggio 2018, data di entrata in vigore del GDPR), Capo VI Documentazione giuridica, art. 1.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

nomi dei genitori o della scuola, che permetterebbero facilmente di risalire all'identità del minore.

2) È altrettanto protetta l'identità "delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone".

3) Resta fermo il divieto posto dall'art. 734 bis del Codice penale alla divulgazione delle generalità o dell'immagine delle vittime di violenza sessuale, senza il loro consenso.

Infine, l'art. 52 prevede la possibile omissione delle generalità degli interessati dalle riproduzioni delle sentenze, nel caso l'interessato faccia una motivata richiesta, per motivi legittimi, nei modi e tempi indicati nell'articolo. Nel caso che l'autorità che emette la sentenza accolga l'istanza di omissione delle generalità,

> "all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: 'In caso di diffusione omettere le generalità e gli altri dati identificativi di...'".

Il divieto alla divulgazione di dati che permettono l'identificazione delle vittime di violenza sessuale posto dal Codice penale non è limitato al contesto della pubblicazione delle sentenze, ma incide su qualunque tipo di divulgazione, anche di tipo giornalistico, e non è limitato alle sole generalità e immagini, ma si estende anche ad informazioni che permettono di identificare la vittima "quanto meno da parte della comunità del luogo nel quale si è verificata l'azione criminosa"[35]. Tale divieto si applica dunque, ovviamente, anche alla eventuale diffusione di riproduzioni di fascicoli processuali, a cui dovrebbe essere analogamente esteso anche l'obbligo di omettere dati che permettono l'identificazione di minori o "delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone".

Nel caso di trattamento a fini di documentazione, studio e ricerca delle riproduzioni dei fascicoli processuali, le norme a garanzia dei diritti degli interessati previste per la pubblicazione delle sentenze sono necessarie ma non sufficienti, perché i fascicoli processuali spesso contengono molte informazioni che non rivestono interesse pubblico, compreso dati su terzi coinvolti a vario titolo nel procedimento giudiziario; possono inoltre più facilmente contenere dati personali di natura

[35] Garante per la protezione dei dati personali, Provvedimento del 25 luglio 2018, n. 432.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

sensibile o sensibilissima, come ad esempio certificati medici o analisi del DNA.[36] Vale la pena di ricordare, per inciso, che il Codice protezione dati personali vieta tassativamente la diffusione dei dati genetici, biometrici e relativi alla salute (art. 2-septies, c. 8); la Cassazione ha stabilito che tale divieto prevale rispetto alle disposizioni dell'art. 52 in merito alla pubblicazione delle sentenze[37].

Allo scopo di offrire adeguate tutele ai diritti e alle libertà degli interessati, si può fare ricorso a misure già presenti nel Codice protezione dati personali e in primo luogo alla distinzione tra comunicazione e diffusione (art. 2-ter, c. 4, lett. a) e b)). Con la prima, s'intende "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato (…)" (come avviene, ad esempio, nelle sale di consultazione di un archivio); con la seconda, s'intende "il dare conoscenza dei dati personali a soggetti indeterminati (…)" (come avviene quando si pubblica una informazione in un libro o in rete). Autorizzare il trattamento delle copie dei fascicoli processuali da parte di un centro studi, non vuol dire autorizzare a diffonderne indiscriminatamente tutti i contenuti *urbi et orbi*. A seconda dei casi, si può prevedere che le riproduzioni dei documenti processuali siano consultabili solo in situ; o siano pubblicate on line con accorgimenti tecnici che ne impediscano la indicizzazione da parte dei motori di ricerca; o si può prevedere che siano pubblicate in aree dei siti web accessibili solo agli utenti registrati.

Anche il Codice dei beni culturali e del paesaggio prevede norme a tutela delle persone a cui si riferiscono i dati personali contenuti nei documenti d'archivio ed in primis norme sulla consultabilità dei documenti. Tali norme però si applicano ai documenti conservati negli archivi dello Stato e degli enti pubblici, nonché negli archivi privati dichiarati di interesse storico particolarmente importante[38]; gli

[36] Ilaria Moroni e Michele di Sivo hanno fornito esempi in tal senso nei loro interventi alla giornata di studi: "La conservazione archivistica nell'era del GDPR: il nodo degli archivi privati e dei dati penali" (Roma, 30 gennaio 2019): www.icar.beniculturali.it/index.php?id=374.

[37] Il caso riguardava una persona che non aveva fatto domanda, ai sensi dell'art. 52, perché venissero omessi i suoi dati identificativi dalla pubblicazione di una sentenza, ma dopo la pubblicazione della sentenza che lo riguardava era ricorso in giudizio perché conteneva informazioni relative alla sua salute. La Cassazione ha affermato che "l'art. 22 Codice Privacy afferma il principio generale per cui i dati sensibilissimi, e specificamente quelli idonei a rivelare lo stato di salute, non possono essere diffusi. Tale indicazione, che non pare ammettere eccezioni, supera il punto di equilibrio indicato dall'art. 52" (Cass. civ., sez. I, 20 maggio 2016, n. 10510).

[38] D. lgs. 196/2003, art. 103. D. lgs. 42/2004, artt. 122-127. Il c. 3 dell'art. 127 contiene un rinvio al c. 3 dell'art. 123 che sembra far intendere che anche agli archivi non dichiarati si applichino le norme

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

archivi privati costituiti da documenti in copia, di cui esistono altrove gli originali, non hanno motivo di essere dichiarati di interesse storico particolarmente importante[39] e quindi nella maggior parte dei casi le riproduzioni dei fascicoli processuali conservate dalle associazioni di familiari o da centri studi sono fuori dal campo di applicazione della norma.

Per gli Archivi di Stato e degli enti pubblici e per gli archivi privati dichiarati di interesse storico particolarmente importante, la legge – oltre ad escludere dalla consultazione per 40 anni, come si è già visto, i dati personali relativi a condanne penali e reati e connesse misure di sicurezza – prevede l'esclusione dalla consultazione per 40 anni dei documenti contenenti dati sensibili e per 70 anni di quelli contenenti dati "idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare" (salvo possibile autorizzazione anticipata alla consultazione, che viene concessa sulla base del progetto di ricerca)[40]. Il decreto del ministro della giustizia, nell'autorizzare il trattamento delle riproduzioni dei fascicoli processuali a scopo di documentazione, studio e ricerca, potrebbe estendere a tali riproduzioni le norme sulla consultabilità che si applicano ai documenti conservati negli Archivi di Stato.

Un altro prezioso strumento per salvaguardare i diritti degli interessati, tutelando allo stesso tempo la libertà di espressione che include "la libertà di ricevere o di comunicare informazioni"[41] sono le *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica*, allegate al Codice protezione dati personali, che gli assegna un ruolo molto importante; infatti "Il rispetto delle disposizioni contenute nelle regole deontologiche (…) costituisce

sulla consultabilità, ma è un errore materiale già segnalato da Paola Carucci, *Consultabilità dei documenti e tutela dei dati personali. Tutela del diritto d'autore e di immagine*, in Paola Carucci e Mariella Guercio, *Manuale di archivistica*, Carocci, Roma, 2008, p. 175, e da Stefano Twardzik, *op.cit.*, pp. 242-43.

[39] La dichiarazione di interesse storico un provvedimento emesso dalle Soprintendenze archivistiche, ai sensi dell'art. 13 del Codice dei beni culturali, d. lgs. 42/2004, da cui discendono per il proprietario obblighi di conservazione ed altri oneri e onori.

[40] Artt. 122 - 127 del D.lgs. 42/2004. Sulla autorizzazione anticipata alla consultazione decide il Ministero dell'interno, udita la Commissione per le questioni inerenti alla consultabilità degli atti di archivio riservati, di cui fanno parte, tra gli altri, un docente universitario di storia, il soprintendente dell'Archivio centrale dello Stato, e un rappresentante del Garante.

[41] *Carta dei diritti fondamentali dell'Unione Europea*, art. 11; tra i diritti fondamentali tutelati dalla Carta è inclusa la "Protezione dei dati di carattere personale" (art. 8).

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

condizione essenziale per la liceità e la correttezza del trattamento dei dati personali"[42].

Le Regole impongono precisi obblighi sia a chi conserva e gestisce gli archivi, sia a chi accede "per scopi storici a documenti contenenti dati personali, anche per finalità giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero" (art. 2). Tanto gli uni quanto gli altri hanno il dovere di trattare i dati personali in modo da garantire la dignità delle persone a cui si riferiscono. Inoltre "L'utente può diffondere i dati personali se pertinenti e indispensabili alla ricerca e se gli stessi non ledono la dignità e la riservatezza delle persone." (art. 11, c. 4). Allo stesso tempo, le Regole deontologiche affermano che "L´interpretazione dell´utente, nel rispetto del diritto alla riservatezza, del diritto all´identità personale e della dignità degli interessati, rientra nella sfera della libertà di parola e di manifestazione del pensiero costituzionalmente garantite." (art. 11, c.1). In breve, le Regole deontologiche sono state in grado di trovare un buon punto di equilibrio tra diversi interessi costituzionalmente tutelati, ed offrono solide garanzie a tutela degli interessati, senza comprimere irragionevolmente il diritto alla ricerca. Ad archivisti ed utenti degli archivi privati utilizzati per scopi storici è fatto obbligo di osservare le Regole deontologiche, anche se l'archivio non è stato dichiarato di interesse storico particolarmente importante[43]. Sembrerebbe comunque opportuno ribadire l'obbligo dell'osservanza delle Regole deontologiche da parte di centri studi o associazioni di familiari autorizzati al trattamento dei dati personali penali.

Alle associazioni di familiari che conservano copie di atti processuali e altri documenti relativi a mafia o terrorismo si attagliano senz'altro le *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica.* Per quanto riguarda i loro utenti, però, il quadro è più complesso, perché l'attività di ricerca sotto alcuni punti di vista è disciplinata da queste stesse regole deontologiche che si applicano a chi consulta archivi sia

[42] Art. 2-quater, c. 4, del D lgs. 196/2003.
[43] D. lgs 42/2004, art. 127, comma 3.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

pubblici che privati[44], mentre da altri punti di vista è disciplinata dalle regole deontologiche per l'attività giornalistica.

Occorre considerare, a questo proposito, che il GDPR ha esteso le deroghe finalizzate a bilanciare la protezione dei dati personali con la libertà di espressione. Mentre la direttiva 95/46/CE (e di conseguenza anche la normativa nazionale) prevedeva deroghe solo nel caso di trattamenti per scopi giornalistici o di "espressione artistica o letteraria" (art. 9), il GDPR prevede deroghe anche in caso di "espressione accademica" (art. 85). Cosa si intenda esattamente con questa locuzione non è chiaro, perché non viene definita; e ancor meno chiari sono i confini tra i trattamenti a fini di ricerca storica e quelli a scopo di "espressione accademica".

L'inclusione nel GDPR della deroga a favore della "espressione accademica" sembra sia stata il frutto di una battaglia condotta dal mondo accademico britannico, ed in particolare dallo Economic and Social Research Council (ESRC) e da Wellcome Trust[45]. Une delle voci più attive è stata quella del giurista dell'università di Oxford David Erdos, che ha denunciato come fosse paradossale che le deroghe a tutela della libertà di espressione della direttiva 95/46/CE permettessero il trattamento dei dati sensibili e penali da parte di chi scriveva sui tabloid (in quanto attività giornalistica), ma non da parte di scienziati sociali che producevano ponderosi saggi su riviste accademiche [46].

In esecuzione dell'art. 85 del GDPR, il D.lgs. 196/2003 – novellato dal D. lgs 101/2018 – oggi dunque permette il trattamento di dati personali penali non solo

[44] Ai sensi dell'art. 126, c. 3 del D.lgs. 22/01/2004, n. 42 Codice dei beni culturali e del paesaggio, "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." L'art. 127 c. 3, estende l'applicazione di questa norma anche agli "archivi privati utilizzati per scopi storici" non dichiarati di interesse storico particolarmente importante.

[45] Questa battaglia è ricordata nel documento *British Academy and ESRC press for shields for Humanities and Social Science Scholarship as UK Implements the new EU General Data Protection Regulation (GDPR),* 13 luglio 2017, on line sul sito della British Academy.

[46] David Erdos, *Freedom of Expression Turned On Its Head? Academic Social Research and Journalism in the European Privacy Framework*, in "Public Law", 2013, n. 1, pp. 52-73. David Erdos, *From the Scylla of Restriction to the Charybdis of Licence? Exploring the scope of the "special purposes" freedom of expression shield in European data protection* in "Common Market Law Review", 2015, vol. 52, n. 1, pp. 119-153. Più di recente, Erdos è tornato su questo tema in una conferenza su "The impact of the GDPR in academic research", nell'ambito del convegno "The Impact of the GDPR in Higher Education" (Imperial College London, 22 June 2017); l'intervento di Erdos è disponibile on line sia in video che in trascrizione.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

per scopi giornalistici, ma anche quando "finalizzato esclusivamente alla pubblicazione o diffusione anche occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'*espressione accademica*, artistica e letteraria". (art. 136, c. 1, lett. c; corsivo aggiunto).

In questi casi, è permesso il trattamento dei dati sensibili (le "categorie particolari di dati" di cui all'art. 9 del GDPR) e dei "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza" anche senza il consenso dell'interessato, purché nel rispetto delle regole deontologiche relative all'attività giornalistica (art. 137, c. 1).

Tali regole deontologiche, secondo il Codice, sono relative non solo ad attività giornalistiche, ma anche ad "altre manifestazioni del pensiero"[47]. Tuttavia è previsto che siano adottate dall'Ordine nazionale dei giornalisti ed il testo delle regole attualmente in vigore sembra riferirsi solo all'attività giornalistica. Il Garante stesso ne auspica l'aggiornamento[48] e sarebbe opportuno che ––aggiornandole ––si prevedessero norme più esplicitamente relative ai trattamenti a fine di "espressione accademica" e/o si chiarisse in che misura le disposizioni si applicano anche all'attività di ricerca nelle scienze umane e sociali.

Ad esempio, le Regole deontologiche dispongono che "Il giornalista che raccoglie notizie" per trattare dati personali

> "rende note la propria identità, la propria professione e le finalità della raccolta salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; evita artifici e pressioni indebite. Fatta palese tale attività, il giornalista non è tenuto a fornire gli altri elementi dell´informativa"[49] (art. 2, c. 1).

Questa norma si applica anche nel caso di osservazione partecipante o di intervista condotta nel corso di una ricerca sociologica o antropologica? La domanda si pone anche perché, a differenza delle regole deontologiche per giornalisti, quelle per archivisti e storici prevedono regole più stringenti per ciò che concerne la raccolta

[47] Nell'ambito del titolo XII *Giornalismo, libertà di informazione e di espressione*, il Capo II, che include l'art. 139 relativo alle regole deontologiche, reca la rubrica *Regole deontologiche relative ad attività giornalistiche e ad altre manifestazioni del pensiero*.

[48] Si vedano le considerazioni in premessa alla Regole.

[49] Ci si riferisce alle informazioni che il titolare del trattamento dei dati personali è tenuto a fornire all'interessato, ai sensi degli artt. 13 e 14 del GDPR.

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

di fonti orali: "In caso di trattamento di fonti orali, è necessario che gli intervistati abbiano espresso il proprio consenso in modo esplicito, eventualmente in forma verbale". (art. 8, c. 1)

La revisione delle regole deontologiche potrà chiarire questi interrogativi. Sarà opportuno che le associazioni rappresentative degli studiosi di scienze umane e sociali si attivino per partecipare alle consultazioni in materia che il Garante attiverà[50].

5. Conclusioni

Nell'era di internet, è necessario garantire alle persone il controllo sui dati che li riguardano, al fine di tutelare il libero sviluppo della persona umana. Per questo, la Carta dei diritti fondamentali dell'Unione Europea include uno specifico articolo sulla protezione dei dati personali (art. 8). Allo stesso tempo, la Carta protegge la libertà di espressione, che include il diritto a ricevere informazioni (art. 11), nonché la ricerca e la "libertà accademica" (art. 13).

Il GDPR affida al diritto degli Stati membri il compito di conciliare questi diversi diritti. In Italia~~,~~ abbiamo già strumenti utili a conciliare la protezione dei dati personali con la libertà di espressione e di ricerca, primi fra tutti le regole deontologiche allegate al Codice per la protezione dei dati personali.

Uno degli ambiti in cui il GDPR affida agli Stati membri un compito specifico di regolamentazione è il trattamento dei "dati personali relativi a condanne penali e a reati e a connesse misure di sicurezza", legittimo solo se autorizzato dal diritto degli Stati membri. La *ratio* della norma è proteggere le persone da usi di tali dati di carattere discriminatorio, estorsivo, o che impediscono il reinserimento sociale di chi ha pagato il proprio debito con la giustizia, e così via. Il pericolo di usi inappropriati dei dati personali penali è alto, come gli esempi statunitensi dimostrano, e giustifica pienamente la severità della norma.

[50] "Lo schema di regole deontologiche è sottoposto a consultazione pubblica per almeno sessanta giorni" (art. 2-quater, c. 2, del D. lgs 196/2003).

Cross Vol.4 N°4 (2018) - DOI: http://dx.doi.org/10.13130/cross-11272

La finalità della norma non è, però, scoraggiare l'attività di organizzazioni della società civile che promuovono la conoscenza dei fenomeni criminali, al fine di combatterli, o che sostengono le battaglie per ottenere giustizia condotte dalle vittime di crimini. È quindi ragionevole chiedere che il ministro della giustizia autorizzi i trattamenti di dati personali penali da parte di questo genere di organizzazioni e per queste tipologie di finalità. Già esistono gli strumenti per assicurare che i trattamenti di dati personali siano effettuati garantendo il rispetto della dignità, dei diritti e della libertà delle persone a cui si riferiscono i dati, basta prevederne l'applicazione anche in questo ambito.

Bibliografia

Nota: I siti web e documenti on line citati erano tutti consultabili il 3 febbraio 2019.

Acosta Luis, *The right to respect for private life: digital challenges, a comparative-law perspective: the United States*, European Parliamentary Research Service, Brussels, 2018.

British Academy and ESRC press for shields for Humanities and Social Science Scholarship as UK Implements the new EU General Data Protection Regulation (GDPR), 13 luglio 2017, www.thebritishacademy.ac.uk/news/british-academy-and-esrc-press-shields-humanities-and-social-sciences-new-eu-data-protection.

Canada Federal Court (Ottawa), A.T. vs. Globe24h.com and Sebastian Radulescu, 2017 CF 114 (CanLII), canlii.ca/t/h31qn.

Carucci Paola, *Consultabilità dei documenti e tutela dei dati personali. Tutela del diritto d'autore e di immagine*, in Paola Carucci e Mariella Guercio, *Manuale di archivistica*, Carocci, Roma, 2008, pp. 165-184.

Cassazione civile, sez. I, sentenza 20 maggio 2016, n. 10510.

Corda Alessandro, *Beyond Totem and Taboo: Toward a Narrowing of American Criminal Record Exceptionalism*, in "Federal Sentencing Reporter", 2018, vol. 30, nn. 4-5, pp. 241-251.

Corda Alessandro, *More Justice and Less Harm: Reinventing Access to Criminal History Records* in "Howard Law Journal" 2016, vol. 60, n. 1, pp. 1-60.

Déziel Pierre–Luc, *Le droit à l'oubli au Canada: l'affaire Globe24h et le rôle du juge dans les requêtes de déréférencement*, in *The Right to be Forgotten in Europe and Beyond / Le droit à l'oubli en Europe et au- delà*, Olivia Tambou, Sam Bourton (Eds.), Blogdroiteuropéen, Luxembourg, 2018, pp. 106-8. Liberamente accessibile alla url: wp.me/p6OBGR-2QK.

Erdos David, *Freedom of Expression Turned On Its Head? Academic Social Research and Journalism in the European Privacy Framework*, in "Public Law", 2013, n. 1, pp. 52-73.

Erdos David*, From the Scylla of Restriction to the Charybdis of Licence? Exploring the scope of the "special purposes" freedom of expression shield in European data protection,* in "Common Market Law Review", 2015, vol. 52, n. 1, pp. 119-153.

Garante per la protezione dei dati personali, Autorizzazione n. 7/2016, *Autorizzazione al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici*, 15 dicembre 2016.

Garante per la protezione dei dati personali, *Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica,* 2 dicembre 2010 (Gazzetta Ufficiale n. 2 del 4 gennaio 2011).

Garante per la protezione dei dati personali, *Provvedimento* 15 giugno 2017, n. 267.

Garante per la protezione dei dati personali, *Provvedimento* 22 maggio 2018, n.317.

Garante per la protezione dei dati personali, *Provvedimento* 25 luglio 2018, n. 432.

International Council on Archives, *Code of Ethics*, Adopted by the General Assembly in its XIIIth session in Beijing (China) on 6 September 1996.

International Council on Archives, *Principles of Access to Archives*, Adopted by the AGM on August 24, 2012.

Moroni, Ilaria, *Terrorismi e mafie: una storia ancora da scrivere #9maggio*, in "Il Mondo degli archivi", 8 maggio 2017, www.ilmondodegliarchivi.org/component/content/article?id=498:terrorismi-e-mafie-una-storia-ancora-da-scrivere-9maggio.

Rete degli archivi per non dimenticare. Guida alle fonti per una storia ancora da scrivere, Ilaria Moroni (a cura di), Istituto centrale per il restauro e la conservazione del patrimonio archivistico e librario, Roma, 2010.

Slane Andrea, *Information Brokers, Fairness, and Privacy in Publicly Accessible Information*, in "Canadian Journal of Comparative and Contemporary Law" 2018, vol. 4, n. 1, pp. 249-291.

Twardzik Stefano, *La consultabilità dei documenti*, in *Archivistica. Teorie, metodi, pratiche*, Linda Giuva e Maria Guercio (a cura di), Carocci, Roma, 2014, pp. 237-261.