Francesco Midiri

Protezione dei dati personali nell'archiviazione e catalogazione del patrimonio culturale

(doi: 10.7390/99474)

Aedon (ISSN 1127-1345)
Fascicolo 3, settembre-dicembre 2020

Ente di afferenza:
()

Aedon
Rivista di arti e diritto *on line*
quadrimestrale diretto da Marco Cammelli

numero 3, 2020, issn 1127-1345 Home Indice Ricerca Risorse web

La digitalizzazione del patrimonio culturale

Protezione dei dati personali nell'archiviazione e catalogazione del patrimonio culturale

di *Francesco Midiri*

Protection of personal data in the archiving and cataloging of cultural heritage
The study first of all defines a general framework of the European and national rules on the processing of personal data created through catalogs aimed at achieving public and general interests (not necessarily aimed at carrying out historical research purposes). Subsequently, the conditions and limits to the processing of the data of the persons to whom the recorded data refer, of the persons who process the catalogues and of the users of the cataloged information are specifically identified. The result of the paper is a series of changes to the ministerial digital catalogs that are necessary to ensure compliance with *data protection* regulations.

Keywords: Archiving Cultural Heritage; Cataloging Cultural Heritage; Personal Data Protection.

1. Inquadramento normativo generale della *data protection*

L'ordinamento europeo ha modificato la disciplina della protezione dei dati personali con il Regolamento del Parlamento europeo e del Consiglio 27 aprile 2016, n. 679 c.d. GDPR, *Global data protection regulation*) senza peraltro alterare l'impianto generale della precedente direttiva del Parlamento europeo e del Consiglio, 24 ottobre 1995, n. 46. La nuova normativa è molto articolata, ma delinea un meccanismo di protezione abbastanza semplice, diretto a garantire che lo sfruttamento dei dati rispetti i diritti fondamentali della persona [1].

In altri termini, la disciplina non protegge un indeterminato valore di impenetrabilità della sfera personale, assimilabile alla *privacy* di stampo anglosassone. Essa, invece, garantisce che il trattamento dei dati personali non avvenga attraverso modalità che comprimano in maniera significativa i diritti inviolabili della persona, anche e soprattutto, quelli non direttamente connessi alla dimensione informativa. Il diritto alla protezione dei dati personali, quindi, si identifica, non nella inconoscibilità di fatti riconducibili alla vita dell'individuo, ma nella pretesa a che i propri dati vengano utilizzati osservando una serie di forme giuridiche considerate per definizione strumentali alla tutela dei diritti fondamentali. In questo senso, la pretesa stessa si distingue in maniera netta dal diritto alla riservatezza.

I dati, innanzitutto, possono essere lecitamente utilizzati solo in presenza di una serie di presupposti di fatto o di diritto, c.d. basi giuridiche, tra le quali abbiamo, ad esempio, il consenso dell'interessato, l'esecuzione di un rapporto contrattuale da lui richiesto, la realizzazione di un rilevante e legittimo interesse giuridico, ma anche l'attuazione di un obbligo di legge, la realizzazione di un'attività di interesse pubblico o l'esercizio di un potere pubblico [2].

Lo sfruttamento delle informazioni, inoltre, deve avvenire secondo una serie di modalità determinate: in maniera lecita (cioè per svolgere attività consentite dall'ordinamento generale), trasparente e corretta, per finalità determinate e non generiche, servendosi dei dati strettamente necessari ed esatti, che debbono essere conservati in modo sicuro e poi cancellati appena possibile [3].

Il sistema si completa con il riconoscimento di una serie di diritti dell'interessato (essere dettagliatamente informato sul trattamento, potere accedere ai propri dati conservati da altri, ottenerne la cancellazione o la rettifica, limitare o vietare il loro ulteriore trattamento se illecito ecc.) e di obblighi dell'utilizzatore, definito titolare o responsabile di trattamento, che sono stati implementati dal regolamento (tenere un registro dei trattamenti, un manuale di trattamento, adottare misure di sicurezza tecnologica contro la violazione dei dati, monitorare preventivamente il rischio di violazione dei diritti, nominare un *data protection officer* ecc.) [4].

Il quadro si chiude con l'implicita valorizzazione di alcuni principi necessari all'effettuazione del trattamento in maniera

lecita: la responsabilizzazione di chi utilizza i dati e la c.d. *privacy by default e by design*, cioè la protezione dei diritti inviolabili dell'interessato fin dalla predisposizione degli apparati organizzativi e tecnologici di utilizzo delle informazioni e, successivamente, nella fase del loro impiego e implementazione [5]. A questo proposito, l'art. 25 stabilisce che, già nella fase di progettazione dei trattamenti, deve essere garantito l'utilizzo delle sole informazioni necessarie e la minimizzazione dei dati fino alla loro pseudonimizzazione. Inoltre, si prevede che "per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica".

Un dato da sottolineare, ancora, è che il GDPR, adottando una nozione oggettiva di funzione pubblica, prevede un regime di protezione dei dati personali unitario, sia per i soggetti pubblici che per quelli privati. Naturalmente, il regolamento consente agli Stati di disciplinare i compiti di interesse generale anche introducendo regole specifiche di protezione dei dati. Il tutto, però, senza alterare l'impianto europeo, cioè osservando, nelle deroghe, il limite della proporzionalità (art. 6, co. 2 e 3 GDPR). Il legislatore sovranazionale, ad esempio, ammette specificamente questa possibilità in materia di particolari categorie di dati (definiti nella nostra tradizione "sensibili") [6] o per attività di trattamento pubbliche particolarmente rischiose per le persone interessate (prevedendo in questo caso un ruolo regolatorio delle Autorità indipendenti nazionali) [7].

In questo quadro, la disciplina europea contempla particolari prescrizioni in materia di registrazione e divulgazione di dati per ragioni di interesse pubblico, che interessano direttamente la nostra materia e che analizzeremo in seguito. Fin d'ora, però, possiamo ricordare la lett. *b*) del paragrafo 1 dell'art. 5 che afferma che i dati personali debbono essere "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ('limitazione della finalità')". In sostanza, l'archiviazione nell'interesse pubblico è una finalità jolly sempre ammessa in trattamenti effettuati per ragioni originariamente differenti.

Il legislatore italiano, con il d.lg. 10 agosto 2018, n. 101, ha adeguato il vecchio Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196) al GDPR [8]. Con riferimento alle attività di interesse generale, l'art. 2-*ter* riafferma il principio di legalità, oltreché per la disciplina delle funzioni, anche per le operazioni di trattamento dei dati (compresa la loro comunicazione a soggetti pubblici che svolgono funzioni pubbliche o a privati). Inoltre, l'art. 2-*quater*, per le stesse attività, consente al Garante di adottare regole "deontologiche" il cui rispetto "costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali". Sono confermate, poi, specifiche regole di attuazione, nonostante il carattere autoapplicativo del Regolamento, in materie come la sanità, l'istruzione, ecc. [9] ed anche in materia di attività di registrazione ed archiviazione [10].

All'interno di queste coordinate normative si collocano i Cataloghi digitali del Mibac, che identificheremo specificamente poco oltre, previsti da una serie di atti ministeriali (decreto ministro Beni culturali 7 ottobre 2008 [11], decreto ministro Beni culturali 23 gennaio 2017 [12], circolare ministro Beni culturali n. 3263 del 30 novembre 2012 [13]) la cui finalità pubblica di catalogazione e digitalizzazione rientra, secondo le indicazioni della stessa amministrazione, nella *mission* di tutela e valorizzazione fondata sugli artt. 3 e 6 del Codice dei beni culturali [14].

Dal contenuto dei cataloghi emergono essenzialmente tre ipotesi di trattamento di dati personali che, come vedremo, devono essere regolate dalla disciplina di *data protection* (talvolta insieme ad altri tipi di regole): le informazioni delle persone fisiche a cui sono variamente attribuiti i beni censiti; quelle di coloro che hanno elaborato le schede; quelle dei fruitori.

2. La disciplina di *data protection* applicabile alle attività di archiviazione e catalogazione

All'interno di queste coordinate generali il GDPR contempla una serie di disposizioni relative al trattamento di dati personali realizzato attraverso le attività di archiviazione, o meglio, seguendo la terminologia delle regole europee, attraverso attività qualificabili in senso più ampio come di registrazione/catalogazione.

Il regolamento, al considerando 158, da un lato, attraverso una formulazione che, nella traduzione italiana, perde chiarezza [15], dà una definizione ampia di questo tipo di trattamenti, identificati nei "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 con un valore a lungo termine per l'interesse pubblico generale"; dall'altro, li assoggetta alle regole europee di *data protection*, stabilendo che "qualora i dati personali siano trattati a fini di archiviazione, il presente regolamento dovrebbe applicarsi anche a tale tipo di trattamento".

Si consideri che la definizione del GDPR conferma quella elaborata dalla giurisprudenza UE sulla scorta della direttiva del 1994, che identificava l'archivio come qualsiasi sistema di dati catalogati, cioè "strutturati secondo criteri specifici che consentono, in pratica, di recuperarli facilmente per un successivo impiego" [16].

Nell'articolato del regolamento, oltre alla definizione di archivio, sono previste una serie di regole relative alle catalogazioni che, in parte riconfermano le disposizioni generali di protezione dei dati, in parte introducono prescrizioni innovative.

Possiamo anticipare fin da ora che i cataloghi del Mibact che saranno esaminati rientrano a pieno titolo nella fattispecie comunitaria dei trattamenti a fini di archiviazione e catalogazione e, quindi, sono assoggettati alle relative prescrizioni europee. Più precisamente, si tratta, in primo luogo, di una banca dati che contempla 30 diverse tipologie di beni SIGECweb), con cui l'Istituto generale per il catalogo e la documentazione, istituito presso il ministero dei Beni culturali (ICCD), gestisce il complesso delle informazioni catalografiche sul patrimonio culturale e, quindi, di una sua versione pubblica on line (Catalogo generale dei beni culturali). L'attività di catalogazione pare riconducibile all'art. 17, in materia di tutela, del Codice dei beni culturali, d.lg. 22 gennaio 2004, n. 42. Alla formazione di questo sistema di catalogazione partecipano amministrazioni pubbliche di varia natura, da autonomie locali ad autonomie funzionali, e alle informazioni possono accedere enti pubblici e privati attivi nel sistema culturale. La versione pubblica, più limitata quantitativamente,

è aperta, invece, alla generalità degli utenti [17].

Tornando alle regole sostanziali europee, l'art. 89, innanzitutto, riafferma l'applicabilità generale delle regole del GDPR anche al "trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici". Inoltre, stabilisce, per le attività di catalogazione, l'applicabilità del principio classico di minimizzazione dei dati, che implica l'utilizzo delle sole informazioni necessarie e che può giungere ad imporre la loro pseudonimizzazione e cancellazione quando non siano più indispensabili per raggiungere le finalità per le quali esse vengono utilizzate [18]. In sostanza, il legislatore europeo ritiene che tutte queste misure siano pienamente applicabili anche ai trattamenti a fini di registrazione nel pubblico interesse e che possano rappresentare, soprattutto la pseudonimizzazione e l'anonimizzazione, soluzioni in grado di garantire *ex se* il rispetto dei diritti degli interessati.

L'art. 89, però, contiene anche una disposizione più propriamente innovativa. Al par. 3 si afferma che "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 ... 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". I classici diritti dell'interessato (accesso, rettifica, cancellazione ecc. ...), quindi, possono essere limitati dalla normativa attuativa se in grado di pregiudicare l'efficacia della funzione pubblica, che nel giudizio del GDPR appare prevalente.

È appena il caso di considerare come nel regolamento si trovino altre disposizioni in materia di archivi che, però, non sono rilevanti per la nostra materia. In particolare, l'art. 5, par. 1 lett. *b*) ed *e*) consente che i dati personali, originariamente raccolti per finalità o tempi determinati, possano sempre essere utilizzati anche "a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" e possano essere, in quest'ultimo caso, "conservati per periodi più lunghi". In altri termini, l'archiviazione nel pubblico interesse può sempre sovrapporsi a differenti finalità di utilizzo dei dati per sfruttarne le relative acquisizioni informative e conservarle senza limiti temporali [19].

Nel nostro caso, peraltro, queste disposizioni generano solamente un *iter* circolare. Infatti, anche l'originaria raccolta di informazioni personali collegate ai beni censiti non digitalmente ha finalità di archiviazione a lungo termine, proprio come la formazione successiva di cataloghi digitali (compresi quello pubblico), che, semmai, si risolve semplicemente nel creare strumenti divulgativi maggiormente accessibili. In altri termini, se volessimo identificare in maniera più sistematica le originarie finalità della formazione dei primi archivi non digitali e del successivo SIGECweb (nonché i tempi di conservazione dei dati), ci renderemmo conto che sono le stesse: la tutela e la valorizzazione dei beni culturali censiti per il tempo della loro esistenza, ed anche oltre [20].

Il sistema normativo del GDPR è stato attuato in Italia, anche con riferimento alle funzioni di archiviazione/catalogazione nell'interesse pubblico, dal Codice sulla protezione dei dati personali, così come riformato del d.lg. 10 agosto 2018, n. 101.

Innanzitutto, l'art. 2-*ter*, al primo comma, stabilisce che la base giuridica rappresentata per il regolamento dai compiti di interesse pubblico o connessi all'esercizio di un pubblico potere, "è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento". Il terzo comma, invece, stabilisce che "la diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1" [21].

Le due disposizioni, in realtà, non fanno altro che trasporre nella disciplina nazionale il principio di legalità dell'azione amministrativa, sia con riferimento a funzioni pubbliche che si realizzano attraverso il trattamento dei dati personali sia con riferimento a quelle che ne implicano la diffusione.

Il Codice, peraltro, contempla anche il Titolo VII della Parte II che disciplina i "Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" e che attua, attraverso il suo art. 97, le disposizioni dell'art. 89 del GDPR che abbiamo già visto.

Alcune norme del Titolo, innanzitutto, riprendono semplicemente le indicazioni del GDPR. Si pensi all'art. 99, che conferma il dettato dell'art. 5 del regolamento europeo (che come abbiamo visto non pare direttamente rilevante nella nostra materia) per affermare che l'utilizzo dei dati a fini di archiviazione nell'interesse pubblico (e la loro cessione) può avere luogo anche dopo la cessazione di un eventuale precedente trattamento realizzato per differenti funzioni. Inoltre, l'art. 101, al comma 2, riafferma il principio generale di necessità e pertinenza dei dati registrati.

Altre disposizioni, invece, forse per la loro fattura tecnica, si distanziano dalle regole europee, creando problemi interpretativi ed applicativi. Il primo comma dell'art. 101, ad esempio, afferma che "i dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 5 del regolamento". La disposizione sembra affermare che gli archivi non possono essere utilizzati come bagaglio informativo per realizzare funzioni ablatorie o sanzionatorie se non nel caso in cui essi siano già destinati ad altre finalità ulteriori rispetto a quelle "primarie" di registrazione e catalogazione per fini storici, culturali ecc. In sostanza, l'apertura degli archivi a finalità almeno duplici consente il loro utilizzo per ogni genere di poteri restrittivi delle situazioni soggettive delle persone.

Tutto questo riverbera inevitabilmente sul principio di necessità e di minimizzazione dei dati, perché il fatto che i dati personali archiviati possano essere usati per molte mission pubbliche eterogenee rende necessaria la registrazione di contenuti informativi tendenzialmente aperti, ampi e "slegati" da funzioni amministrative predeterminate *ex ante*. E questo fa correre il rischio di svuotare i principi normativi comunitari e di entrare in conflitto con le regole del GDPR [22].

Nella nostra materia, peraltro, questi problemi applicativi possono essere evitati ritenendo che la catalogazione del Mibact sia realizzata esclusivamente nel pubblico interesse unitario della tutela e della valorizzazione dei beni culturali e non, invece, per altre e differenti funzioni amministrative. In questo modo, i dati registrati non potrebbero essere aperti ad ulteriori attività ablatorie e, per questo, non potrebbero essere sottratte di fatto ai principi di necessità e minimizzazione europei.

Ulteriore disposizione problematica è il terzo comma dell'art. 101 che stabilisce che i dati personali degli archivi possono "essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico". Per questo, le informazioni potrebbero essere disseminate anche in cataloghi digitali aperti.

La disposizione integra, come norma di specie, quella dell'art. 2-*ter* del Codice che impone un rigido principio di legalità per l'utilizzo pubblico delle informazioni personali. Tuttavia, pare eccessiva nel facoltizzare i trattamenti.

Nel nostro caso, ad esempio, l'attribuibilità della proprietà di un bene può essere stata fornita in adempimento di un obbligo di legge, si pensi ad una richiesta di autorizzazione a fini di manutenzione o restauro o ad una dichiarazione a fini fiscali. Il canone del comportamento pubblico rivelatore della seconda parte della norma, poi, è sfuggente. Ad esempio, può essere considerato tale il semplice utilizzo non occulto o dissimulato di un immobile vincolato? In sostanza, anche questa disposizione pare potere porre problemi di compatibilità con le regole del GDPR, perché attraverso norme attuative in materia di funzioni di catalogazione pare introdurre nuovi presupposti di liceità del trattamento non riconducibili alle regole europee, quali appunto una sorta di consenso implicito al trattamento per comportamenti concludenti.

Da ultimo, si consideri che lo stesso Codice dei beni culturali (d.lg. 22 gennaio 2004, n. 42), agli artt. da 122 a 127, contiene alcune disposizioni in materia di dati personali trattati in archivi pubblici. Gran parte di esse, peraltro, ponendo una serie di limiti all'ostensibilità di dati di norma non registrati o diffusi nei Cataloghi Mibact, (quali dati sensibili, giudiziari e secretati per ragioni di politica estera o interna di Stato), non appaiono direttamente rilevanti [23].

L'art. 126, invece, disciplina il diritto del "titolare dei dati" a bloccarne l'utilizzo quando questi ultimi "non siano di rilevante interesse pubblico", ed "il loro trattamento comporti un concreto pericolo di lesione della dignità, della riservatezza o dell'identità personale dell'interessato". La disposizione, che, nonostante la lettera, fa riferimento all'"interessato" al trattamento e al suo "diritto di opposizione" comunitario, pare essere ormai superata dalla normativa del GDPR. Infatti, se nella sua prima parte sembra alludere al principio di necessità di trattamento (di cui all'art. 5 dello stesso GDPR), nella seconda parte pone una serie di presupposti e limiti al diritto di opposizione che il regolamento del 2018 non prevede, stabilendo che l'opposizione al trattamento di interesse pubblico possa essere esercitata semplicemente "per motivi connessi alla sua situazione particolare" (art. 21 prima parte) [24].

L'ultimo comma dell'art. 126, poi, afferma 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". Si tratta di un mero rinvio che va riferito oggi, nella nuova disciplina europea e nella sua attuazione italiana, alle c.d. Regole deontologiche previste dal nuovo Codice in materia di protezione dei dati personali all'art. 20.

A questo proposito, si tenga conto che il Garante italiano ha emanato le "Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica", provvedimento n. 513 del 19 dicembre 2018 [25], che, peraltro, paiono fare riferimento ad una fattispecie differente rispetto alla nostra materia, nella quale non si tratta di archiviare e consultare dati esclusivamente a fini storici, ma di trattare i dati personali per esigenze di tutela e valorizzazione dei beni culturali (anche quando nel Catalogo generale si converte la base dati di archivio SIGECweb in strumenti digitali di diffusione e consultazione delle informazioni aperti a tutti) [26].

Per concludere, la visione di insieme di questo panorama ci dice che la normativa europea estende alle attività di catalogazione di interesse pubblico i principi normativi generali della *data protection* e le garanzie dei diritti rappresentate dalla minimizzazione dei dati. La normativa italiana, invece, introduce alcuni elementi di rigidità rappresentati dalla rigorosa predeterminazione legislativa delle finalità pubbliche di registrazione dei dati e da limiti generali alla diffusione delle informazioni.

3. La disciplina di *data protection* relativa ai dati delle persone fisiche a cui appartengono, od a cui sono riconducibili a vario titolo i beni censiti

La disciplina di *data protection* regola, innanzitutto, la catalogazione dei dati delle persone fisiche viventi, menzionate nei cataloghi del Mibact, alle quali sono riconducibili i beni culturali. Si tratta di tutte quelle informazioni relative a coloro che esercitano diritti sulle cose censite o che, a vario titolo, sono menzionati nelle narrazioni storiche o nelle note di ogni genere contenute nelle schede di archivio. Più in generale, si fa riferimento a tutte le indicazioni relative alla sfera personale di soggetti determinati che possono essere tratte dalla descrizione fisica, storica o giuridica delle *res* catalogate. In tutti questi casi, la registrazione digitale rappresenta a pieno titolo, una forma di "trattamento" che rientra nella fattispecie definitoria dell'art. 4 del GDPR [27].

In questo caso, la funzione della normativa di *data protection* è quella di impedire che le modalità di realizzazione di una funzione pubblica pregiudichino in maniera rilevante, senza la giustificazione del perseguimento di un interesse generale, i diritti inviolabili delle persone menzionate nei cataloghi. Si pensi al diritto alla sicurezza ed alla integrità del patrimonio personale che potrebbero essere messi in pericolo dalla indicazione della titolarità proprietaria e dalla collocazione dei beni catalogati. La disciplina, in questo caso, opera attivando una serie di istituti che dovrebbero rendere proporzionata e sostenibile l'azione amministrativa.

Come abbiamo visto, anche l'utilizzo di questo tipo di informazioni ricade nell'applicazione della regola generale dell'art.

25 del regolamento - relativo alla *privacy by design e by default* - e della sua attuazione specifica in materia di cataloghi dell'art. 89.

Per questo, anche i nostri registri di pubblico interesse, proprio come tutte le altre forme di trattamento organizzate, osservano il principio secondo il quale debbono essere utilizzate soltanto informazioni strettamente necessarie e, anche in quest'ultimo caso, debbono essere adottate forme di minimizzazione e pseudonimizzazione dei dati. Soprattutto quando i trattamenti possano porre a rischio i diritti e le libertà fondamentali degli interessati.

Inoltre, non pare potersi escludere l'applicazione di quella regola generale dell'art. 25, richiamata sopra e che non risulta superata dalle regole speciali, secondo la quale la diffusione dei dati ad un numero indeterminato di destinatari deve avvenire in esito all'"intervento della persona fisica".

Date queste coordinate normative, i riferimenti delle persone a cui sono attribuiti i beni potranno essere diffusi attraverso i cataloghi solo nel caso in cui questa forma di trattamento risulti necessaria, sulla scorta di considerazioni squisitamente tecnico-operative di ambito culturale, per la realizzazione delle finalità di tutela e valorizzazione dei beni culturali censiti.

Anche in quest'ultimo caso, peraltro, si dovrà considerare l'opportunità di adottare criteri di pseudonimizzazione ed anonimizzazione, indicando, ad esempio, la riconducibilità del bene ad un "proprietario privato" genericamente inteso, piuttosto che ad una persona identificata nominalmente. In questo modo, si forniranno alcune informazioni, quali la titolarità proprietaria di un soggetto fisico non identificato, che potranno caratterizzare il bene senza porre a rischio i diritti dell'interessato. In sostanza, la menzione dell'identità si imporrà solo nel caso in cui essa stessa qualifichi sul piano storico culturale il bene ai fini della sua tutela e valorizzazione.

In ogni caso, si dovrà applicare l'ultima parte dell'art. 25 che impone l'intervento dell'interessato per ogni forma di diffusione di dati. Si tenga conto, infatti, che, con riguardo ai trattamenti realizzati attraverso i cataloghi digitali Mibact, il trattamento non consiste nell'acquisizione e nella conservazione di dati in archivi, ma nella diffusione, cioè nella comunicazione dell'informazione a una platea tendenzialmente indifferenziata ed aperta di destinatari. Tale intervento, poi, che non sarà sicuramente rappresentato da un consenso, non previsto come condizione di liceità per un trattamento nell'interesse pubblico dall'art. 6, si tradurrà in una forma di partecipazione analoga a quella della legge 7 agosto 1990, n. 241 per l'azione amministrativa.

Oltre alle disposizioni del GDPR, peraltro, anche il Codice italiano contiene prescrizioni che paiono rilevanti per i nostri cataloghi.

Più precisamente, l'art. 2-*ter*, come abbiamo visto, prevede, in generale, una riserva di legge relativa (con una base giuridica costituita da legge o da regolamento nei soli casi previsti da legge) per ogni attività di rilievo pubblico che importi il trattamento dei dati e, in particolare, per la "la diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità".

Nel nostro caso, la diffusione dei dati realizzata dai cataloghi digitali non pare essere sostenuta da un adeguato fondamento legislativo, essendo prevista solo da decreti ministeriali (il d.m. beni culturali 7 ottobre 2008 e sue modificazioni già citato), e, per questo, potrebbe essere ritenuta illecita.

La disposizione italiana, particolarmente rigorosa, rappresenta una deroga nazionale alla normativa europea ammessa dall'art. 6, commi 2 e 3 del GDPR, per garantire l'efficacia dei trattamenti di interesse pubblico, a patto che sia conforme ai canoni di proporzionalità. Per considerare pienamente leciti i nostri trattamenti e consentirne l'operatività pare necessario disapplicare la regola nazionale, considerandola non proporzionata alle sue finalità ed alla protezione dei diritti degli interessati, per ritornare alle disposizioni generali più permissive del GDPR.

A questo proposito, sulla scorta della giurisprudenza europea maturata sulla base di prescrizioni pur differenti (quelle della direttiva del 1995 che rimetteva agli Stati la disciplina delle funzioni di interesse pubblico per realizzare le quali risultava lecito trattare i dati personali anche senza consenso), è possibile affermare che le deroghe legislative nazionali siano proporzionate quando "forzino" le modalità normative di trattamento per garantire l'efficacia dell'azione amministrativa [28]. Per usare i termini della nostra costituzione, per realizzare il buon andamento dell'art. 97. Ed in questo quadro, è appena il caso di considerare che la stessa giurisprudenza esclude che i legislatori nazionali possano sostanzialmente introdurre "requisiti supplementari" per il trattamento dei dati [29].

La deroga del nuovo Codice, invece, rafforzando le posizioni soggettive degli interessati, naturalmente tendenti a limitare la diffusione di informazioni personali, pare perseguire il differente valore dell'imparzialità dello stesso art. 97. In questo modo, però, il legislatore nazionale, più che proporre modifiche all'impianto europeo non proporzionate, si propone addirittura un obiettivo diverso rispetto a quello dell'efficacia dell'azione pubblica, unica condizione che, per il GDPR, consente agli Stati di introdurre deroghe normative.

A questo punto, è possibile affermare che il regime complessivo posto in luce dovrà essere applicato anche con riferimento a due diverse fattispecie di trattamento di dati personali assimilabili a quella analizzata, che, allo stato, facendo riferimento al sito del SIGECweb e del Catalogo aperto, non vengono realizzate, ma che potrebbero esserlo in seguito: la riproduzione fotografica di persone viventi (quale ritratto fotografico o no) [30] e la trasmissione di informazioni di persone viventi in eventuali schede riepilogative di vicende storiche del bene culturale.

È possibile considerare, infine, che le indicazioni contenute nelle schede possono contemplare informazioni relative a defunti. A questo proposito, il considerando 27 del GDPR afferma che "*il presente regolamento non si applica ai dati personali delle persone decedute*" ma, nel medesimo tempo, consente agli Stati di "*prevedere norme riguardanti il trattamento dei dati personali delle persone decedute*". Il legislatore italiano ha sfruttato la clausola di garanzia e, seguendo la precedente regolazione del Garante [31], ha previsto una forma di tutela relativa a questo tipo di dati.

Infatti, nell'art. 2-terdecies, il Codice riformato nel 2018, per quanto di nostro interesse, ha stabilito che "*i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*". In altri termini, un ventaglio ampio di soggetti è in grado di utilizzare, con riferimento a questo tipo di informazioni, gli strumenti correttivi "classici" (accesso, rettifica, limitazione di utilizzo, cancellazione, portabilità e opposizione al trattamento), previsti dal GDPR, per reintegrare *ex post* la correttezza giuridica, in senso lato, dello sfruttamento dei dati.

Dal tenore letterale delle disposizioni richiamate del legislatore europeo pare che agli interessati sia consentito esercitare una sorta di intervento "puntiforme" sulle informazioni divulgate, essenzialmente per conoscerle o eliminarle, in tutto od in parte. Non sembra ammesso, invece, intervenire per condizionare la discrezionalità (tecnica od amministrativa), esercitata dall'amministrazione nella strutturazione degli archivi, per ricondurla alla piena osservanza della *privacy by design e by default* di cui all'art. 25 del GDPR. Cosa che, invece, gli interessati viventi possono ottenere, con riferimento al trattamento dei propri dati, rivolgendosi al giudice ordinario, ai sensi dell'art. 150 del Codice, per richiedere la piena applicazione dell'intera normativa di *data protection* [32].

Va anche considerato, poi, che, talvolta, dati direttamente inerenti a persone defunte possono assumere la veste di informazioni che interessano indirettamente persone viventi. Ad esempio, la falsa attribuzione ad un proprietario defunto di un bene culturale censito può tradursi nel dato personale dell'ipotetica trasmissione della sua titolarità in capo agli eredi necessari.

A latere di tutte queste considerazioni si deve ricordare che, nel caso in cui vengano diffusi dati personali di soggetti legati ai beni censiti, indipendentemente dalla necessità del loro consenso, è necessario fornire loro un'adeguata informativa, ai sensi degli artt. 13 e 14 del GDPR (si tenga conto a questo riguardo che obbligo di richiedere il consenso se necessario ed obbligo di fornire la informativa sono rigidamente separati nella nuova come nella vecchio disciplina di *data protection*).

È appena il caso di ricordare che il nuovo regolamento europeo ha implementato i precedenti obblighi di informazione e ne ha introdotti di nuovi. Il tutto nel quadro di principi generali di trasparenza, semplicità ed accessibilità delle informative. In particolare, come avremo modo di vedere anche per il trattamento dei dati degli utenti, è necessario fornire una serie di dati importanti, come la base giuridica e le finalità del trattamento, i tempi di conservazione dei dati, i riferimenti del responsabile della protezione dei dati, eventuali forme di profilazione, i diritti anche di reclamo degli interessati [33].

Con riferimento alla nostra materia, peraltro, l'art. 14 par. 5 del regolamento esclude l'obbligo di informativa nel caso in cui "comunicare tali informazioni (quelle della informativa) risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici... In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni". Come abbiamo visto, il trattamento effettuato attraverso i cataloghi del Mibact non realizza, *stricto sensu*, soltanto una forma di archiviazione, ma, semmai, anche di diffusione dei dati archiviati. Tuttavia, paiono esistere le condizioni per applicare estensivamente la disposizione. In questo senso, pare possibile dare corso ad informative semplificate realizzate attraverso il sito internet, proprio come avviene, come vedremo, per i dati personali degli utenti che accedono ai cataloghi digitali.

4. La disciplina di *data protection* relativa ai dati degli autori delle schede

Le informazioni relative agli autori delle schede non sono propriamente riconducibili al bene culturale censito, inteso come substrato fisico funzionale alla realizzazione di un interesse pubblico. In altri termini, si tratta di dati relativi alla formazione della scheda nella sua identità di documento rappresentativo e descrittivo della cosa catalogata, cioè a dati relativi alle modalità di realizzazione di un'attività amministrativa di servizio pubblico. Per questo, a differenza dei dati delle persone a cui sono legati i beni culturali, essi non paiono potere rientrare nel novero delle indicazioni che debbono essere diffuse attraverso i cataloghi digitali per realizzare le funzioni di tutela e di valorizzazione dei beni stessi.

Questa forma di trattamento, invece, pare potere essere ricondotta alle regole generali del GDPR (non quelle relative a cataloghi ed archivi) ed alle regole nazionali sulla trasparenza dell'azione pubblica.

Anche in questo caso, come per i dati delle persone menzionate nei cataloghi, l'obiettivo della disciplina è quello di garantire che il trattamento dei dati, anche per la realizzazione della prevalente funzione pubblica di trasparenza, non sia in grado di pregiudicare, per le sue modalità di realizzazione, i diritti inviolabili dell'interessato.

A questo riguardo, si consideri che l'art. 86 della fonte europea attribuisce agli stati nazionali la disciplina dell'accesso ai loro atti amministrativi che importi il trattamento di informazioni soggettive, vincolandoli, peraltro, all'obbligo di "conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento" [34].

La diffusione dei dati degli autori delle schede, quindi, deve avvenire secondo i presupposti e le condizioni di liceità fissate dal legislatore comunitario che abbiamo già indicato, ma anche secondo le regole di trasparenza della nostra legislazione, poste essenzialmente dal d.lg. 14 marzo 2013, n. 33.

Alla luce di questa disciplina, la diffusione dei dati degli autori delle schede può essere qualificata come una forma di pubblicazione facoltativa dell'amministrazione - non essendo riconducibile a specifici obblighi legislativi - come tale soggetta alla disposizione dell'art. 7-*bis*, secondo il quale "le pubbliche amministrazioni possono disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare ai sensi del presente decreto o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5-*bis*, procedendo alla indicazione in forma anonima dei dati personali eventualmente presenti".

Anche in questo caso, siamo di fronte, ai sensi dell'art. 86 del regolamento, a una deroga alla normativa comunitaria che impone l'anonimizzazione dei dati personali nelle pubblicazioni facoltative, senza condizioni, come garanzia dei diritti degli interessati. I cataloghi del Mibact, allora, non potranno comunicare i nominativi degli autori delle schede, ma, qualora si rendesse necessario per la realizzazione della trasparenza, potranno fornire informazioni differenti che non consentano, peraltro, di ricostruire l'identità del funzionario [35].

Proprio come per i nominativi delle persone a cui sono riconducibili i beni censiti, per disapplicare la rigida norma italiana e ritornare alle più permissive regole generali europee si dovrà considerarla anticomunitaria.

In questo caso, però, proprio perché il legislatore europeo non consente deroghe per la migliore efficacia delle funzioni amministrative, ma per contemperare le ragioni di una mission pubblica con le posizioni soggettive delle persone coinvolte dalla sua realizzazione - per tornare alla nostra tradizione giuridica per perseguire le ragioni della imparzialità - la disapplicazione pare problematica. Infatti, nel decreto trasparenza il legislatore nazionale intende proprio dare corso a quest'ultimo compito, attraverso scelte essenzialmente politiche che paiono attaccabili solo sul fronte della loro ragionevolezza.

Peraltro, una volta eliminato tramite disapplicazione l'art. 7-*bis* del Codice dal sistema normativo italiano, non saranno di ostacolo alla diffusione dei dati degli autori delle schede i limiti dell'accesso civico dell'art. 5-*bis* del d.lg. n. 33 del 2013 (relativo alla diversa fattispecie della pretesa all'ostensione di dati non originariamente pubblicati), primo fra tutti quello della "protezione dei dati personali, in conformità con la disciplina legislativa in materia". La disciplina complessiva della *data protection*, infatti, privata dei vincoli rigorosi dell'art. 7-*bis* del Codice, consente la divulgazione anche di questo tipo di dati [36], pur nell'osservanza di una serie di principi [37].

5. La disciplina di *data protection* relativa ai dati personali degli utenti

Come abbiamo visto, anche il trattamento dei dati degli utenti è oggetto della regolamentazione ad opera della disciplina generale europea. Anche in questo caso, la funzione della normativa è quella di consentire solamente il trattamento dei dati strettamente necessario all'accesso ad un servizio pubblico, evitando ulteriori forme di conservazione, elaborazione od utilizzo delle informazioni che possano pregiudicare le libertà fondamentali dei fruitori del servizio. Si pensi a fenomeni di tracciamento dei loro orientamenti culturali, delle loro preferenze, della loro estrazione sociale o dei loro interessi.

Le modalità di trattamento dei dati degli utenti sono illustrate dall'informativa fornita sul sito dello stesso catalogo generale del Mibact [38]. È ragionevole pensare che si tratti delle stesse modalità adottate per gli utenti del SIGECweb. Peraltro, questi ultimi paiono essere essenzialmente persone giuridiche, come tali prive del diritto alla protezione dei dati personali secondo la normativa europea.

Occorre innanzitutto considerare che le informazioni vengono fornite dal ministero facendo espresso riferimento all'adempimento degli obblighi dettati dal precedente Codice in materia di protezione dei dati personali ed all'attività della precedente agenzia di regolazione europea (il Gruppo di lavoro art. 29) [39]. Per questo è lecito ritenere che l'intera prassi di trattamento delle informazioni personali, oltre all'informativa, siano modellate sulla base del precedente regime e, quindi, debbano essere adeguate al nuovo GDPR.

In questa sede, allora, si debbono fornire alcune indicazioni relative all'adeguamento della informativa sul trattamento dei dati, che costituisce il momento di contatto primario tra chi utilizza i dati e gli interessati, ma anche alla *compliance* complessiva alla nuova normativa.

La disciplina degli obblighi di informazione o trasparenza è oggi contenuta negli art. 13 e 14 del GDPR e trovano un'autorevole interpretazione nelle Linee guida sulla trasparenza ai sensi del regolamento 2016/679 adottate dal Gruppo di lavoro art. 29 in data 29 novembre 2017 WP260 rev.01 (con *endorsement* della nuova autorità European *data protection board*) [40].

Il documento ministeriale, come vedremo, proprio perché adottato in ottemperanza della precedente normativa, richiede alcuni adeguamenti.

Innanzitutto, con riguardo ai soggetti che utilizzano le informazioni personali degli utenti, l'informativa pubblicata identifica nell'"Istituto centrale per catalogo e la documentazione" il titolare del trattamento dei dati, cioè il soggetto/organismo che determina le finalità ed i mezzi del trattamento.

Successivamente, però, con riferimento al luogo del trattamento, l'informativa diventa meno chiara nell'identificazione dei destinatari dei dati, cioè dei soggetti a cui questi ultimi vengono comunicati. In particolare, dopo avere chiarito che i dati non sono diffusi (cioè non sono comunicati ad una platea indifferenziata di destinatari) si afferma che i "trattamenti" possono "essere curati ... dai responsabili designati dal titolare". È probabile che si faccia riferimento ai capi degli organi o degli uffici deputati alla gestione delle informazioni, cioè a soggetti interni al ministero, ma lo si fa utilizzando una categoria giuridica, quella dei responsabili del trattamento, che, nel GDPR, ha un significato diverso. Si tratta delle persone fisiche o giuridiche (o gli organismi), differenti rispetto al titolare, ma che trattano i dati per conto di quest'ultimo (di norma si tratta di trattamenti in outsourcing realizzati in forza di un contratto). Utilizzando il concetto di responsabile inteso in questi termini, i dati personali verrebbero comunicati dall'organismo che gestisce il catalogo a soggetti terzi non meglio identificati [41].

Ancora, sempre nella stessa parte del documento si afferma che i dati personali forniti dagli utenti per avere informazioni o fornire suggerimenti "sono eventualmente comunicati ad altri soggetti pubblici o privati nel solo caso in cui ciò sia necessario per fornire le informazioni da Voi richieste", soggetti che non vengono identificati neppure come categorie generali (ad esempio per tipologia operativa quali istituzioni di cultura, enti locali, fondazioni bancarie, enti del terzo settore) come, invece, imporrebbe la nuova normativa.

In sostanza, la prima revisione dell'informativa da operare è quella di identificare con maggiore chiarezza il titolare ed i responsabili o le categorie di responsabili del trattamento, soprattutto fornendo con maggiore precisione i dati di contatto (fornendo numeri di telefono ed indirizzi di posta elettronica e non solo indirizzi). E questo soprattutto nel caso in cui, come spesso accade, la gestione delle infrastrutture informative che hanno memoria dei dati avvenga con la collaborazione di tecnici esterni utilizzati in outsourcing che possono accedere ai dati stessi e divengono, quindi, responsabili di trattamento.

Più in generale, peraltro, è necessario chiarire i ruoli e le competenze di tutti gli organismi che, nel quadro della gestione dei cataloghi digitali, sono chiamati a svolgere funzioni di trattamento, e qualificarli correttamente in titolari, responsabili ed incaricati [42] secondo le definizioni del GDPR [43].

In questo quadro, peraltro, l'informativa deve indicare, ai sensi dell'art. 14 del regolamento, l'identità ed i dati di contatto della nuova figura del responsabile della protezione dei dati personali (il *data protection officer* del GDPR) che, ai sensi della nuova normativa europea, deve essere sempre designato quando "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico" [44], come nel nostro caso [45].

Il sito dei cataloghi identifica, poi, in maniera chiara, una prima tipologia di dati trattati, specificando che si tratta di informazioni "la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet" che si sostanziano in "parametri relativi al sistema operativo e all'ambiente informatico dell'utente" [46]. Corretta appare anche l'indicazione secondo la quale eventuali comunicazioni di posta elettronica consentono l'acquisizione del nominativo e dell'indirizzo mail [47].

Anche le finalità del trattamento, per questi dati, sono indicate in maniera adeguata nella necessità di "controllare il corretto funzionamento del sistema" [48].

Meno chiaro, invece, il tempo di conservazione dei dati, infatti, da un lato, si afferma che questi vengono immediatamente cancellati, dall'altro, si afferma che gli stessi possono essere utilizzati, evidentemente in un momento successivo, per fare valere eventuali responsabilità per reati informatici dell'utente. In tale modo, poi, si afferma, implicitamente, una nuova finalità di trattamento. È lecito pensare, ancora, che i dati possano essere utilizzati anche per fare valere forme di responsabilità civile, senza alcuna informativa in merito.

Successivamente, poi, il documento informa che viene trattata un'ulteriore tipologia di dati, cioè i dati personali forniti dagli utenti nei moduli di registrazione per fruire dei servizi del sito. In questo caso, le informazioni avrebbero dovuto essere più chiare, ed avrebbero dovuto indicare, in maniera più specifica, i tipi di dati necessari per accedere ai servizi ulteriori rispetto alla mera consultazione del sito, le finalità di utilizzo ed i tempi di conservazione.

Occorre considerare, inoltre, che, con riguardo alla tipologia dei dati trattati, alle finalità ed ai tempi di utilizzo, siamo di fronte ad un'informativa a due facce: per i dati personali tecnici le indicazioni sono sostanzialmente conformi alla nuova normativa, per i dati personali di accesso ai servizi, invece, le indicazioni debbono essere senz'altro implementate.

A questo riguardo, su di un piano generale, è necessario che l'Istituto che gestisce i cataloghi elabori una policy, (o in altri termini un documento regolatorio interno), nella quale vengano identificati con precisione, tipologie di dati personali, finalità e basi giuridiche di utilizzo, tempi di conservazione ecc. Si tratta di un adempimento fondamentale per dare corso ai principi di responsabilizzazione e di riduzione del rischio di violazione dei diritti degli interessati che traspaiono dal tessuto normativo del GDPR.

Ancora, nella parte dell'informativa più propriamente dirette a chiarire le "modalità del trattamento", si indica genericamente che i dati sono conservati per il tempo necessario a realizzare le finalità per le quali sono stati raccolti (indicazione che come detto avrebbe dovuto essere posta nelle parti precedenti), e, soprattutto, che sono adottate misure di sicurezza ad evitare la loro perdita o il loro uso illecito o non corretto.

A questo proposito, con riguardo all'approntamento delle misure di sicurezza per evitare "violazioni di dati personali" (c.d. *data breach*), il GDPR ha operato una svolta, prevedendo, all'art. 32, che queste ultime non debbano essere imposte *ex ante* dai legislatori nazionali o dalle autorità di regolazione, ma debbano essere elaborate dagli stessi titolari, sulla base della loro analisi dei rischi. Questa operazione assume il carattere di elemento fondamentale del principio di responsabilizzazione di chi tratta i dati (c.d. *accountability*) e si riverbera, per così dire, nella redazione dell'informativa che deve fornire indicazioni adeguatamente articolate proprio sulle soluzioni organizzative e tecniche in grado di ostacolare la dispersione dei dati [49].

Anche in questo senso, quindi, il documento ministeriale andrebbe integrato. Ma, soprattutto, dovranno essere elaborate, in relazione al rischio di lesione dei diritti degli interessati attraverso la violazione dei dati personali, soluzioni tecniche ed organizzative adeguate [50].

L'informativa si chiude, anche in questo caso sinteticamente, indicando i diritti degli interessati, facendo però riferimento alla precedente normativa codicistica italiana. La materia, invece, è stata assunta dal GDPR che ha riarticolato ed implementato, pur nella falsariga della normativa precedente, le pretese soggettive degli interessati [51].

Per queste ragioni, l'informativa, adeguata al tempo della sua elaborazione, andrebbe forse arricchita in questa parte, o, comunque, riferita all'impianto del nuovo regolamento. Allo stesso modo la struttura organizzativa del ministero dovrà essere adeguata per rendere effettivo l'esercizio dei diritti, prevedendo, tra l'altro, la nomina di un *data protection officer*.

Come abbiamo visto, l'esigenza di integrare l'informativa deriva dalla necessità di adeguarne i contenuti alla nuova normativa. A questo proposito, occorre considerare che il GDPR contempla nuovi obblighi di informazione e non solo un'implementazione degli obblighi precedenti. Il regolamento, infatti, impone i principi di trasparenza, di accessibilità e

di semplicità per ogni fattispecie di trattamento e, a più forte ragione, per l'informativa [52]. Si rende necessario, quindi, fornire le informazioni del caso in maniera esauriente e articolata, evitando di pregiudicare la "leggibilità" attraverso tecnicismi. Ciò pare condurre ad informative più lunghe, schematiche ed esemplificative.

Procedendo in ordine di importanza nell'indicazione dei nuovi obblighi, il regolamento impone di chiarire approfonditamente le finalità del trattamento. Si tratta delle ragioni per cui i dati vengono utilizzati e con riguardo alle quali si deve indicare la normativa che giustifica e rende necessario l'utilizzo delle informazioni lecito e necessario.

Nel medesimo tempo, il legislatore europeo impone di indicare la base giuridica del trattamento, cioè la situazione di fatto o di diritto che costituisce il presupposto necessario e sufficiente per effettuare lecitamente il trattamento ai sensi dell'art. 6 (l'esecuzione di un contratto richiesta dall'interessato, l'adempimento di un obbligo di legge, la realizzazione di un legittimo interesse del titolare ecc.).

Occorre considerare che, ai sensi dell'art. 6, co. 3, GDPR, nel caso di un trattamento svolto per realizzare un compito pubblico la finalità e la base giuridica coincidono. In altri termini, l'obiettivo di chi realizza una funzione pubblica è dare esecuzione alla regola che la contempla come attività di interesse generale.

In ogni caso, a questo proposito, l'informativa ministeriale dovrà essere integrata per indicare come fine/presupposto del trattamento dei dati degli utenti il regolare funzionamento dei siti dei cataloghi necessario alla realizzazione delle funzioni pubbliche di tutela e di valorizzazione dei beni censiti (come indicato nel sito nella presentazione dei cataloghi nella informativa) stabilite dalla legge. In ossequio al principio di trasparenza, poi, potrebbe essere anche utile chiarire quali specifici compiti di interesse pubblico riconducibili al Codice dei beni culturali vengono realizzati attraverso il trattamento dei dati dei cataloghi Mibact.

Come abbiamo già indicato, peraltro, tutto quanto attiene alle finalità e alle basi giuridiche dovrà essere oggetto di una specifica regolamentazione interna conforme al GDPR.

Infine, il regolamento ha imposto di indicare con chiarezza se i dati possano essere trasferiti a soggetti collocati fuori dal territorio dell'Unione europea, cosa che non avviene nel nostro caso, semplificando di molto il tenore di un'integrazione all'informativa.

6. Obblighi generali imposti dal GDPR con riguardo ad ogni forma di trattamento realizzata attraverso i cataloghi del Mibact

A questo punto della analisi è possibile porre in evidenza, pur senza alcuna pretesa di completezza, alcuni obblighi generali introdotti dal GDPR che possono valere con riferimento ad ogni forma di trattamento di dati personali realizzata attraverso i cataloghi del Mibact: da quelli delle persone collegati ai beni censiti, ai dati dei dipendenti pubblici ed a quelli degli utenti.

Si tratta, anche in questo caso, di regole che proteggono l'integrità dei diritti inviolabili degli interessati che possano essere pregiudicati dalle concrete modalità di utilizzo delle informazioni per la realizzazione di una funzione di interesse generale.

In via generale, come abbiamo visto, si impongono i principi di *privacy by default e by design* che derivano dall'art. 25 del regolamento che prescrivono "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso" di ridurre i rischi di violazione dei diritti degli interessati, pur riconoscendo le prerogative di sfruttamento lecito delle informazioni.

Tutto ciò impone, come abbiamo già visto, di minimizzare il trattamento dei dati personali e di effettuarlo entro rigidi canoni di necessità per la realizzazione delle finalità pubbliche dei cataloghi. Ma si rende necessario, ai sensi dell'art. 30 del regolamento, elaborare appositi registri di trattamento assimilabili a documenti regolatori interni che specifichino partitamente tutte le modalità di sfruttamento delle informazioni [53]. Con riguardo ai dati degli utenti, in particolare, ciò significa limitarsi a utilizzare dati personali necessari al regolare funzionamento dei cataloghi e, nel caso in cui le informazioni dovessero essere utilizzate per ragioni di marketing o di promozione culturale, determinare precisamente le modalità di sfruttamento e, soprattutto, preoccuparsi di acquisire il consenso degli interessati.

In quest'ottica, ci si dovrà adeguare ai rigidi canoni di trasparenza dell'art. 5, anche agevolando i rapporti con tutti gli interessati attraverso strutture quali responsabili della protezione dei dati, identificati e organizzati sul modello dei responsabili del procedimento di cui alla legge n. 241 del 1990, che garantiscano l'esercizio dei diritti degli interessati (dalle informative ai reclami). Inoltre, ai sensi dell'art. 13 e 14 GDRP, dovranno essere approntate, per ogni ipotesi di trattamento ed indipendentemente dalla esigenza di acquisire il relativo consenso, apposite informative, articolate ma accessibili, in grado di illustrare in maniera esaustiva tutte le condizioni, le modalità e le finalità dell'utilizzo delle informazioni.

Il principio di riservatezza ed adeguatezza dell'art. 5 impone, in termini generali, la previsione di misure tecniche e organizzative adeguate ad evitare le violazioni dei dati personali che possano porre a rischio i diritti degli interessati, si pensi alla divulgazione di dati in ordine alla proprietà od alla collocazione di opera d'arte, ma anche in ordine alle sfere di interesse degli utenti dei registri. Anche in questo caso, le misure, autodeterminate in relazione al principio di responsabilizzazione, dovranno essere specificate in appositi documenti e periodicamente adeguate, ai sensi dell'art. 32 [54]. Fa da pendant a questi obblighi il dovere di notificare alla Autorità garante ogni eventuale forma di violazione dei dati ai sensi dell'art. 33 [55].

Vi sono poi obblighi non direttamente introdotti dal GDPR ma che sono necessari per date attuazione ai vari principi di liceità del trattamento. Si pensi alla necessità di nominare un amministratore di sistema, cioè un soggetto a cui venga attribuita la responsabilità della gestione complessiva della infrastruttura informatica attraverso la quale vengono

trattati i dati, a garanzia della sua sicurezza e della protezione dei diritti [56].

7. Alcune considerazioni conclusive

L'applicazione della disciplina della *data protection*, come abbiamo visto, conduce a due esiti differenti con riferimento ai dati personali dei soggetti riconducibili ai beni censiti (ed alle relative schede) e con riferimento ai dati personali degli utenti dei cataloghi.

Nel primo caso, la normativa europea, attraverso l'applicazione di una serie di principi di liceità di trattamento, primo fra tutti quello di minimizzazione, consente non soltanto l'archiviazione di informazioni personali collegate ai beni censiti ma, anche e soprattutto, la loro diffusione ad una platea indifferenziata di destinatari. Il tutto senza la necessità di alcun consenso degli interessati (ma solo di un loro coinvolgimento partecipativo), visto il carattere oggettivamente pubblico dei trattamenti. La normativa italiana di attuazione, invece, pone vincoli rigidi alla possibilità di trasmettere dati attraverso cataloghi digitali accessibili a tutti. Infatti, con riguardo alle informazioni relative alle persone a cui sono riconducibili i beni censiti, impone il limite di carattere formale rappresentato dal principio della riserva di legge relativa, a fondamento di tutte le attività pubbliche che importino la comunicazione delle informazioni ad una pluralità indifferenziata di destinatari. Ciò conduce a un rilevante ridimensionamento del contenuto dei cataloghi, a meno di non disapplicare la normativa italiana, considerandola incompatibile con quella europea.

A questo riguardo, si consideri che il divieto di comunicare questo tipo di dati attraverso cataloghi digitali non impedisce in assoluto la loro ostensibilità. Per acquisirli si dovranno utilizzare gli strumenti ordinari che nel nostro ordinamento consento l'accesso alle informazioni, anche in questo caso osservando i relativi limiti e divieti, rappresentati essenzialmente dalle norme del Codice dei beni culturali, che abbiamo visto prima, relative alla consultabilità degli archivi.

Con riferimento alle informazioni relative a chi ha elaborato le schede, è la normativa italiana sulla trasparenza, a cui fa rinvio in termini generali il GDPR, ad imporre limiti di carattere sostanziale rappresentati dalla loro anonimizzazione. Anche in questo caso, si avrà una riduzione dell'accessibilità dei cataloghi che potrà essere superata solo disapplicando la normativa italiana.

In sostanza, la normativa italiana di attuazione, utilizza la possibilità di introdurre deroghe nell'interesse pubblico prevista dal regolamento europeo per innalzare significativamente gli standard di protezione dei diritti degli interessati, ritenendo, in questo modo, di non pregiudicare l'efficacia delle funzioni pubbliche di catalogazione digitale, ovvero della tutela e della valorizzazione dei beni culturali. È possibile considerare, peraltro, che il nuovo Codice italiano, ma anche la normativa sulla trasparenza dell'azione amministrativa, avrebbero potuto, nella nostra materia, porre indicazioni maggiormente permissive, valorizzando magari i meccanismi della *privacy by design* e della minimizzazione in considerazione del grado di rischio per i diritti rappresentato dalla diffusione delle informazioni. Si tratta, in ogni caso, di scelte di carattere squisitamente politiche demandate al legislatore nazionale.

Nel secondo caso, cioè con riferimento al trattamento dei dati degli utenti, invece, la normativa europea conferma i suoi classici principi generali di trattamento e quella italiana batte la strada di un sostanziale adeguamento al GDPR, senza introdurre limiti rilevanti, né di ordine formale che sostanziale. In questo senso, si aprono maggiori spazi di sfruttamento delle informazioni, anche se ciò incide in maniera molto relativa sulle modalità di svolgimento delle attività di trattamento dei dati personali attraverso cataloghi digitali di beni culturali e, quindi, sulle funzioni della loro tutela e valorizzazione. In altri termini, viene "liberalizzato" lo sfruttamento delle informazioni degli utenti che accedono ai cataloghi, negli stessi termini in cui ciò avviene per la gran parte dei servizi imprenditoriali e commerciali. Ma questa apertura "a valle", nei rapporti con coloro che accedono ai siti Mibact, non incide sulle logiche e sui contenuti della catalogazione digitale dei beni culturali a fini pubblici, e, quindi, sulle modalità di realizzazione dei compiti amministrativi, che rimangono assoggettati a regole molto più rigide, soprattutto con riguardo alla gamma di informazioni che possono essere trattate e diffuse.

Note

[1] Sul GDPR, v. G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; A. Barba e S. Pagliantini (a cura di) *Delle persone*. *Leggi collegate*, vol. II, in *Commentario al codice civile*, diretto da E. Gabrielli, Milano, 2019; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

[2] GDPR, art. 6.

[3] GDPR, art. 5.

[4] Cfr. i diritti dell'interessato negli artt. 12-22 del GDPR; cfr. gli obblighi di chi tratta i dati negli artt. 30, 32, 35, 36 e 37 del GDPR.

[5] Su questi temi A. Mantelero, *Responsabilità e rischio nel reg. UE 2016/679*, in *Le nuove leggi civili commentate*, 2017, pag. 144; G Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, *ivi*, 2017, 1. Con riferimento all'attività di regolazione europea si consideri European data protection board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 2019, in http://edpb.europa.eu/. In particolare, sul principio di *accountability* cfr. G. Finocchiaro, *Il principio di accountability*, in *Giur. it.*, 2019, pag. 2278.

[6] GDPR, art. 9, co, 2 lett. *g*) e co. 4.

[7] GDPR, art. 36, co. 5.

[8] Sul nuovo Codice italiano, *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, opera diretta da G. Finocchiaro, Bologna, 2019; R. Sciaudone, E. Caravà (a cura di), *Il Codice della privacy: commento al D.*

Lgs. 30 giugno 2003, n. 196 e al D. Lgs. 10 agosto 2018, n. 101 alla luce del Regolamento (UE) 2016/679 (GDPR), Ospedaletto, 2019; G. Cassano *et al.* (a cura di), *Il processo di adeguamento al GDPR: aggiornato al D.lgs. 10 agosto 2018, n. 101*, Milano, 2018; L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del d. lgs. 101/2018*, Milano, 2018.

[9] Parte II, Titoli V, VI.

[10] Parte II, Titolo VII.

[11] In http://www.iccd.beniculturali.it/it/norme-regolamenti-circolari/4221/decreto-ministeriale-2008-ordinamento-dell-istituto-centrale-per-il-catalogo-e-la-documentazione.

[12] In https://www.beniculturali.it/mibac/multimedia/MiBAC/documents/1487863233671_REGISTRATO_REP._37.pdf.

[13] In http://www.iccd.beniculturali.it/it/norme-regolamenti-circolari/4335/circolare-iccd-3263-2012-catalogo-nazionale-dei-beni-culturali_-chiarimenti-e-procedure-per-l-assegnazione-dei-codici-enti-e-dei-numeri-di-catalogo-generale.

[14] Come risulta dal sito del Catalogo http://www.catalogo.beniculturali.it/sigecSSU_FE/visualizzaPagina.action?testoCercato=Catalogo.

[15] A questo riguardo, si richiama la versione inglese del Considerando: "Where personal data are processed for archiving purposes, this Regulation should also apply to that processing, bearing in mind that this Regulation should not apply to deceased persons. Public authorities or public or private bodies that hold records of public interest should be services which, pursuant to Union or Member State law, have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest. Member States should also be authorised to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes".

[16] Sentenza della Corte (Grande Sezione) del 10 luglio 2018 (Causa C-25/17, 2018/C 319/07), in GU C 86 del 20 marzo 2017 ed in https://eur-lex.europa.eu/ ed in *Responsabilità Civile e Previdenza*, 2019, 1, pag. 89, con nota di R. Panetta, *Proselitismo religioso e protezione dei dati personali: tra esigenze di tutela e particolarità della fattispecie*, *ivi*, pag. 101.

[17] Cfr. http://www.iccd.beniculturali.it/it/sigec-web e http://www.catalogo.beniculturali.it/sigecSSU_FE/visualizzaPagina.action?testoCercato=Catalogo.

[18] Sulla disposizione G. Ramaccioni, *Commento all'art. 89*, in *Commentario al codice civile*, cit., *Delle persone*. *Leggi collegate*, vol. II, op. cit.; M.C. Daga, *Le disposizioni relative a specifiche situazioni di trattamento: l'attività di archiviazione e ricerca, il segreto professionale e le associazioni religiose*, in *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, *op. cit.* Ma si vedano anche le linee guida in materia elaborate dall'European Archives Group, struttura della Commissione europea, *Guidelines for the implementation of the General Data Protection Regulation (GDPR) by archive services*, in https://ec.europa.eu/info/files/guidance-data-protection-archive-services_en.

[19] Sulla disposizione D. Achille, *Commento all'art. 5*, in *Commentario del codice civile*, cit., *Delle persone*. *Leggi collegate*, vol. II, *op. cit.*, e sul principio di finalità del trattamento A. D'Ottavio, G. Nava, *Gdpr, il principio di finalità: un equilibrio tra privacy e innovazione*, in *Agenda digitale*, 13 settembre 2018, https://www.agendadigitale.eu/sicurezza/gdpr-il-principio-di-finalita-un-equilibrio-tra-privacy-e-innovazione/ sui principi di trattamento cfr. C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, fasc. 22.

[20] Come risulta dalla pagina web dei cataloghi http://www.catalogo.beniculturali.it/sigecSSU_FE/visualizzaPagina.action?testoCercato=Catalogo.

[21] Sulla disposizione G. Mulazzani, *Il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in *La protezione dei dati personali in Italia: Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, *op. cit.* Nella stessa disposizione troviamo nei termini seguenti la nozione di diffusione e comunicazione dei dati personali nell'esercizio di una funzione pubblica: "4. Si intende per: a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione; b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

[22] Si tenga conto che il legislatore italiano sta utilizzando la possibilità conferita dall'art. 6 del GDPR di specificare le regole di trattamento europee nel caso di funzioni pubbliche. La regola, però, consente una normazione attuativa di specificazione che sia proporzionata alla realizzazione efficace delle *mission* pubbliche e non una normazione derogatoria rispetto alle prescrizioni europee (cosa espressamente ammessa dallo stesso regolamento all'art. 23 solo con riguardo alla limitazione nazionale dei diritti dell'interessato).

[23] Su queste disposizioni G. Manfredi, *Sub Artt. 122-127*, in *Il codice dei beni culturali e del paesaggio*, Bologna, 2004, (a cura di) M. Cammelli e Id., *La nuova disciplina della consultabilità dei documenti degli archivi: gli artt. 122 e 123*, in *Aedon*, 2008, 3.

[24] Si tenga conto che, come abbiamo visto, l'art. 89 del GDPR attribuisce agli Stati la possibilità di porre limiti ai diritti degli interessati con riferimento a trattamenti di dati per finalità di interesse pubblico solamente nel caso in cui questi rischino "*di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità*". Nell'art. 126 del Codice dei beni culturali il rischio di pregiudizio all'interesse pubblico non è neppure menzionato, per questo la disposizione pare essere cedevole rispetto al nuovo regolamento europeo.

[25] doc. web n. 9069661 in www.garanteprivacy.it.

[26] Più precisamente, a questo proposito, l'art. 1 delle Regole afferma: "Le presenti regole riguardano i trattamenti di dati personali effettuati per scopi storici in relazione ai documenti conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico. Le regole deontologiche si applicano, senza necessità di sottoscrizione, all'insieme dei trattamenti di dati personali comunque effettuati dagli utenti per scopi storici".

[27] Analoga considerazione era già stata fatta con riferimento alla precedente normativa da G. Finocchiaro, *La valorizzazione delle opere d'arte on-line e in particolare la diffusione on-line di fotografie di opere d'arte. Profili giuridici*, in *Aedon*, 2009, 2.

[28] Corte giustizia UE sez. II, 27/09/2017, n.73, in *Foro Amm.*, 2017, 9, pag. 1782; Corte Giust. UE, sez. III, 30 maggio 2013,

n. 342, in *Foro it.*, 2013, 12, IV, pag. 522; Corte Giust. UE, grande sezione, 16 dicembre 2008, n. 524, in *Diritto e Giustizia online*, 2008; Corte Giust. UE, 20 maggio 2003, n. 465, in *Europa e dir. priv*., 2004, pag. 691, con nota di S. Mormile.

[29] Per tutte Corte Giust. UE, sez. III, 24 novembre 2011, n. 468, in *Foro amm. - CDS*, 2011, 11, pag. 3281.

[30] Recentemente la Corte di cassazione ha identificato i limiti nei quali la riproduzione fotografica è in grado di proporre, anche indirettamente, informazioni personali: "La neutralità del contenuto dei dati acquisiti senza il consenso della parte committente di una prestazione d'opera, dai quali non si desumano riferimenti alla vita privata o ai beni personali, ma solo alle caratteristiche estetiche e tecniche del manufatto eseguito dall'esecutore dell'opera, esclude che nella condotta assunta, in assenza di preventivo consenso dell'avente diritto, possa ravvedersi una violazione degli obblighi di salvaguardia degli interessi e diritti altrui. Né tantomeno è ravvisabile una violazione del diritto alla privacy, all'immagine o della proprietà altrui nel comportamento di chi, nel proprio personale interesse, acquisisca dati contenenti immagini del proprio manufatto che, se anche riferite a parte del mobilio o degli ambienti in cui esso si inserisce, si dimostrino prive di contenuto personale riferito al committente dell'opera (confermata la sentenza con cui era stata rigettata la domanda di risarcimento che due coniugi avevano proposto nei confronti dell'impresa che loro stessi avevano incaricato del rifacimento degli infissi della villa di loro proprietà. In particolare, i ricorrenti chiedevano il ristoro per il danno non patrimoniale subito in seguito alla pubblicazione di immagini della loro abitazione sul catalogo pubblicitario dell'impresa)", Corte Cass. civile, sez. III, 29 ottobre 2019, n. 27613, in *Guida al diritto*, 2020, 7, pag. 78.

[31] Per tutti cfr. Garante protezione dei dati personali, provv. 19 dicembre 2002, doc web n. 1067167 e Id., provv. 4 aprile 2019, doc. web 9113909, in www.garanteprivacy.it.

[32] In questo senso, sia consentito rinviare a F. Midiri, *Il diritto alla protezione dei dati personali*, Napoli, 2017.

[33] Sugli obblighi di informazione M. Durante, *Commento all'art. 13* e *Commento all'art. 14*, in *Commentario al codice civile*, *op. cit.*; e F. Piraino, *I diritti dell'interessato nel Regolamento generale sulla protezione dei dati personali*, in *Giurisprudenza italiana*, 2019, pag. 2789.

[34] Sul tema sia consentito rinviare a F. Midiri, *GDPR e accesso ai documenti amministrativi*, in *Foro Amm.*, 2018, pag. 2217.

[35] Nelle Linee Guida in materia di trasparenza relative alla originaria versione del d.lg. 33 del 2013 il Garante prevedeva che i dati anonimi contenuti addirittura nelle pubblicazioni obbligatorie dovessero essere resi riutilizzabili dai terzi attraverso licenze di riutilizzo in grado di "*vietare ai titolari delle licenze di re-identificare gli interessati e di assumere qualsiasi decisione o provvedimento che possa riguardarli individualmente sulla base dei dati personali così ottenuti, nonché prevedere in capo ai medesimi titolari l´obbligo di informare l´organismo pubblico nel caso in cui venisse rilevato che gli individui interessati possano essere o siano stati re-identificati*", punto 6 "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" (Pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014) Registro dei provvedimenti n. 243 del 15 maggio 2014 doc. web n. 3134436. La licenza per l'utilizzo delle schede del Catalogo generale dei beni culturali è reperibile al link https://creativecommons.org/licenses/by-nc-sa/2.5/it/ e contempla il limite del riutilizzo a fini commerciali delle immagini o dei dati. Il tema della identificazione degli autori non è contemplato proprio perché direttamente possibile attraverso la lettura delle schede.

[36] Per un recente bilancio sui limiti alla trasparenza in riferimento alla protezione dei dati personali cfr. per tutti E. D'alterio, *Protezione dei dati personali e accesso amministrativo: alla ricerca dell'"ordine segreto"*, in *Giorn. dir. amm.*, 2019, 9.

[37] Con riferimento a limiti e modalità di accesso alle informazioni sul ruolo di un dipendente pubblico nel regime del GDPR si è espresso recentemente il Garante, doc. web n. 9198091, *Parere su una istanza di accesso civico* - 10 ottobre 2019, Registro dei provvedimenti n. 185 del 10 ottobre 2019.

[38] http://www.catalogo.beniculturali.it/sigecSSU_FE/visualizzaPagina.action?testoCercato=Privacy.

[39] Si tratta di Articolo 29 - Gruppo di lavoro per la tutela dei dati personali, *Raccomandazione relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione Europea*, adottata il 17 maggio 2001, WP43, in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1609845.

[40] Cfr. https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_it.

[41] Sulla definizione dei titolari e dei responsabili come autori del trattamento dei dati cfr. A. Mantelero, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it.*, 2019, pag. 2799. Ma vedi anche EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2 settembre 2020, in https://edpb.europa.eu/.

[42] Anche se questa ultima categoria, più chiara nella precedente disciplina, si desume indirettamente dal nuovo GDPR come figura che identifica i soggetti chiamati a operare sui dati per incarico di un titolare o di un responsabile di trattamento. Tale potrebbe essere un soggetto a capo di un ufficio o di un organo che utilizza informazioni personali.

[43] Questo soprattutto con riferimento al complesso quadro di partecipanti alla gestione e di utenti del SIGECweb.

[44] GDPR, art. 37.

[45] Sulla figura F. Lorè, *Il ruolo del responsabile della protezione dei dati personali nella pubblica amministrazione alla luce del regolamento generale sulla protezione dei dati personali UE 2016/679*, in *Amministriv@mente*, 2018, fasc. 7-8.

[46] Cfr. Trattamento dati utenti del catalogo. Si tenga conto che il documento dedica ampio spazio ai c.d. cookies del sito (cookie è lo strumento tecnico attraverso il quale vengono registrate tutte quelle informazioni immesse sul browser allorché si visiti un sito web che trattiene diversi dati come, ad esempio, il nome del server da cui proviene, l'identificatore numerico eccetera) e chiarisce che si tratta che, sostanzialmente ed in maniera atecnica, non conducono alla raccolta di dati personali (si tratta di cookies di sessione o analitici, riconducibili alla figura dei cookies tecnici). Per indicazioni tecniche e giuridiche sui cookies cfr. A. Passaro, C. Ponti, *Privacy e cookie alla luce del GDPR: le soluzioni alle problematiche tecniche e giuridiche* in https://www.cybersecurity360.it/legal/privacy-dati-personali/privacy-e-cookie-post-gdpr-le-soluzioni-alle-problematiche-tecniche-e-giuridiche/.

[47] Correttamente si esclude anche l'acquisizione di dati sensibili e giudiziari.

[48] Cfr. Trattamento dati utenti del catalogo.

[49] In tema per tutti, A. Mantelero, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, *op.*

cit.

[50] Si tenga conto a questo proposito che l'art. 32 GDPR stabilisce che nell'approntare le misure di sicurezza si dovrà tenere conto "in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".

[51] Si pensi, ad esempio, all'accesso al tempo di conservazione dei dati o ad eventuali procedure di profilazione *ex* art. 15 del GDPR.

[52] Si tratta di principi essenzialmente derivabili dall'art. 5 del GDPR.

[53] L. Giacomini, *Il registro delle attività di trattamento previsto dal GDPR: più di uno strumento di mera "compliance"*, in *Rivista di diritto dei media*, 2018, fasc. 3.

[54] Ma anche essere in grado di dimostrare con atti formali all'Autorità l'attività di riduzione del rischio (parere 3/2010 del Gruppo di lavoro articolo 29).

[55] Sulla violazione dei dati personali recentemente M. D'Agostino Panebianco, *Lineamenti di responsabilità derivanti dalla violazione al trattamento dati*, in *Europa e diritto privato*, 2020, pag. 237.

[56] Cfr. Garante per la protezione dei dati personali, *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema* - 27 novembre 2008, doc. web n. 1577499, in *www.garanteprivacy.it*.

.

inizio pagina